

Doc 9859
AN/474



Manuel de gestion de la sécurité (MGS)

Approuvé par le Secrétaire général
et publié sous son autorité

Troisième édition — 2013

Organisation de l'aviation civile internationale

Doc 9859
AN/474



Manuel de gestion de la sécurité (MGS)

**Approuvé par le Secrétaire général
et publié sous son autorité**

Troisième édition — 2013

Organisation de l'aviation civile internationale

Publié séparément en français, en anglais, en arabe, en chinois, en espagnol et en russe par l'ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE
999, rue University, Montréal (Québec) H3C 5H7 Canada

Les formalités de commande et la liste complète des distributeurs officiels et des librairies dépositaires sont affichées sur le site web de l'OACI (www.icao.int).

Première édition, 2006

Deuxième édition, 2009

Troisième édition, 2013

Doc 9859, Manuel de gestion de la sécurité (MGS)

N° de commande : 9859

ISBN 978-92-9249-330-1

© OACI 2013

Tous droits réservés. Il est interdit de reproduire, de stocker dans un système de recherche de données ou de transmettre sous quelque forme ou par quelque moyen que ce soit un passage quelconque de la présente publication, sans avoir obtenu au préalable l'autorisation écrite de l'Organisation de l'aviation civile internationale.

TABLE DES MATIÈRES

	<i>Page</i>
Glossaire	IX
Sigles et abréviations	IX
Définitions.....	XIII
Chapitre 1. Présentation générale du manuel	1-1
1.1 Généralités	1-1
1.2 Objectif	1-1
1.3 Structure.....	1-2
Chapitre 2. Notions fondamentales de gestion de la sécurité	2-1
2.1 Le concept de sécurité	2-1
2.2 L'évolution de la sécurité	2-1
2.3 Causalité des accidents.....	2-3
2.4 Humains, contexte et sécurité	2-7
2.5 Erreurs et violations.....	2-9
2.6 Culture de sécurité	2-11
2.7 Le dilemme de la gestion.....	2-14
2.8 Gestion du changement	2-15
2.9 Intégration des systèmes de gestion	2-16
2.10 Comptes rendus et investigations sur la sécurité	2-17
2.11 Collecte et analyse des données sur la sécurité	2-19
2.12 Indicateurs de sécurité et surveillance des performances.....	2-25
2.13 Dangers.....	2-25
2.14 Risque de sécurité.....	2-28
2.15 Gestion des risques de sécurité	2-32
2.16 Spécifications prescriptives et spécifications fondées sur les performances.....	2-34
Appendice 1 au Chapitre 2. Liste de vérification pour évaluation de la culture de sécurité de l'organisation (OSC)/du profil de risque de l'organisation (ORP) — Exploitants aériens	2-App 1-1
Appendice 2 au Chapitre 2. Exemple de feuille de calcul d'atténuation d'un risque de sécurité	2-App 2-1
Appendice 3 au Chapitre 2. Illustration d'une procédure de priorisation des dangers.....	2-App 3-1
Chapitre 3. SARP de l'OACI relatives à la gestion de la sécurité	3-1
3.1 Introduction.....	3-1
3.2 Spécifications relatives à la gestion de la sécurité par les États.....	3-1

	Page	
3.3	Spécifications relatives à la gestion de la sécurité par les prestataires de services	3-2
3.4	Nouvelle Annexe 19 — <i>Gestion de la sécurité</i>	3-5
Chapitre 4.	Programme national de sécurité (PNS).....	4-1
4.1	Introduction.....	4-1
4.2	Cadre du PNS	4-1
	Composant 1 du PNS. Politique et objectifs de sécurité de l'État.....	4-2
	Élément 1.1 du PNS Cadre législatif de l'État de la sécurité.....	4-2
	Élément 1.2 du PNS Responsabilités et imputabilités de sécurité de l'État	4-3
	Élément 1.3 du PNS Enquête sur les accidents et incidents	4-4
	Élément 1.4 du PNS Politique d'exécution.....	4-4
	Composant 2 du PNS. Gestion de risques de sécurité de l'État.....	4-5
	Élément 2.1 du PNS Exigences en matière de sécurité pour les SGS des fournisseurs de services	4-5
	Élément 2.2 du PNS Accord sur les performances de sécurité des fournisseurs de services	4-6
	Composant 3 du PNS. Assurance de sécurité par l'État	4-6
	Élément 3.1 du PNS Supervision de la sécurité.....	4-7
	Élément 3.2 du PNS Collecte, analyse et échange de données de sécurité	4-7
	Élément 3.3 du PNS Ciblage axé sur les données de sécurité pour la supervision de domaines présentant des problèmes ou des besoins plus importants.....	4-8
	Composant 4 du PNS. Promotion de la sécurité par l'État	4-9
	Élément 4.1 du PNS Formation, communication et diffusion à l'interne des informations de sécurité	4-9
	Élément 4.2 du PNS Formation, communication et diffusion à l'externe des informations de sécurité	4-10
4.3	Planification de la mise en œuvre du PNS	4-11
	4.3.1 Généralités	4-11
	4.3.2 Description du système de réglementation.....	4-11
	4.3.3 Analyse des carences	4-12
	4.3.4 Plan de mise en œuvre du PNS	4-12
	4.3.5 Indicateurs de sécurité	4-12
4.4	Mise en œuvre du PNS — Méthode par étape.....	4-14
	Phase 1	4-15
	Phase 2	4-18
	Phase 3	4-19
	Phase 4	4-21
	Appendice 1 au Chapitre 4. Directives sur l'établissement d'un énoncé de politique nationale sur la sécurité	4-App 1-1
	Appendice 2 au Chapitre 4. Directives sur un système national de compte rendu volontaire et confidentiel	4-App 2-1
	Appendice 3 au Chapitre 4. Exemple de procédure nationale de compte rendu obligatoire	4-App 3-1
	Appendice 4 au Chapitre 4. Indicateurs de performance de sécurité du PNS.....	4-App 4-1

	<i>Page</i>
Appendice 5 au Chapitre 4. Protection des informations de sécurité	4-App 5-1
Appendice 6 au Chapitre 4. Orientations sur la notification et le compte rendu d'accidents et d'incidents	4-App 6-1
Appendice 7 au Chapitre 4. Liste de vérification de l'analyse de l'écart du PNS et plan de mise en œuvre.....	4-App 7-1
Appendice 8 au Chapitre 4. Exemple de contenu d'un document de PNS.....	4-App 8-1
Appendice 9 au Chapitre 4. Exemple de règlement national sur les SGS.....	4-App 9-1
Appendice 10 au Chapitre 4. Exemple de politique nationale d'application.....	4-App 10-1
Appendice 11 au Chapitre 4. Lignes directrices sur les procédures nationales d'exécution dans un environnement PNS-SGS.....	4-App 11-1
Appendice 12 au Chapitre 4. Exemple de liste de vérification d'une acceptation/évaluation réglementaire de SGS.....	4-App 12-1
Chapitre 5. Système de gestion de la sécurité (SGS).....	5-1
5.1 Introduction.....	5-1
5.2 Portée.....	5-1
5.3 Cadre du SGS.....	5-2
Composant 1 du SGS. Politique et objectifs de sécurité	5-3
Élément 1.1 du SGS Engagement et responsabilité de la direction.....	5-3
Élément 1.2 du SGS Obligations de rendre compte en matière de sécurité	5-7
Élément 1.3 du SGS Nomination du personnel clé de sécurité	5-10
Élément 1.4 du SGS Coordination de la planification des interventions d'urgence.....	5-12
Élément 1.5 du SGS Documentation relative au SGS	5-13
Composant 2 du SGS. Gestion des risques de sécurité.....	5-15
Élément 2.1 du SGS Identification des dangers.....	5-15
Élément 2.2 du SGS Évaluation et atténuation des risques de sécurité	5-19
Composant 3 du SGS. Assurance de la sécurité	5-22
Élément 3.1 du SGS Surveillance et mesure de la performance de sécurité.....	5-23
Élément 3.2 du SGS La gestion du changement	5-25
Élément 3.3 du SGS Amélioration continue du SGS	5-26
Composant 4 du SGS. Promotion de la sécurité	5-27
Élément 4.1 du SGS Formation et éducation.....	5-27
Élément 4.2 du SGS La communication relative à la sécurité.....	5-28
5.4 Planification de la mise en œuvre du SGS.....	5-29
5.4.1 Description du système	5-29
5.4.2 Intégration de systèmes de gestion	5-29
5.4.3 Analyse des écarts	5-31
5.4.4 Plan de mise en œuvre du SGS.....	5-32
5.4.5 Indicateurs de performances de sécurité.....	5-32
5.5 Méthode de mise en œuvre par phases	5-33
5.5.1 Généralités	5-33

	<i>Page</i>
5.5.2 Phase 1	5-34
5.5.3 Phase 2	5-37
5.5.4 Phase 3	5-38
5.5.5 Phase 4	5-40
5.5.6 Éléments du SGS mis en œuvre progressivement au cours des Phases 1 à 4	5-41
Appendice 1 au Chapitre 5. Signatures électroniques.....	5-App 1-1
Appendice 2 au Chapitre 5. Description de poste type pour un directeur de la sécurité.....	5-App 2-1
Appendice 3 au Chapitre 5. Planification des interventions d'urgence	5-App 3-1
Appendice 4 au Chapitre 5. Orientations sur l'élaboration d'un manuel SGS.....	5-App 4-1
Appendice 5 au Chapitre 5. Systèmes de comptes rendus volontaires et confidentiels	5-App 5-1
Appendice 6 au Chapitre 5. Indicateurs de performance de sécurité du SGS.....	5-App 6-1
Appendice 7 au Chapitre 5. Liste de vérification pour l'analyse des écarts et plan de mise en œuvre.....	5-App 7-1
Supplément. Éléments d'orientation connexes de l'OACI	Sup-1

GLOSSAIRE

SIGLES ET ABRÉVIATIONS

AAC	Autorité de l'aviation civile [<i>Civil aviation authority (CAA)</i>]
AD	Consigne de navigabilité [<i>Airworthiness directive</i>]
ADREP	Système de comptes rendus d'accident/incident (OACI) [<i>Accident/Incident Data Reporting System (ICAO)</i>]
AIB	Commission d'enquête sur les accidents [<i>Accident investigation board</i>]
AIR	Navigabilité [<i>Airworthiness</i>]
ALoSP	Niveau acceptable de performances de sécurité [<i>Acceptable level of safety performance</i>]
AMAN	Manœuvre brusque [<i>Abrupt manoeuvring</i>]
AME	Technicien de maintenance d'aéronef [<i>Aircraft maintenance engineer</i>]
AMO	Organisme de maintenance agréé [<i>Approved maintenance organization</i>]
AMS	Calendrier de maintenance d'aéronef [<i>Aircraft maintenance schedule</i>]
ANS	Service de navigation aérienne [<i>Air navigation service</i>]
AOC	Certificat d'exploitant aérien [<i>Air operator certificate</i>]
AOG	Aéronef au sol [<i>Aircraft on ground</i>]
AS	Assurance de la sécurité [<i>Safety assurance (SA)</i>]
ASB	Bulletin du service d'alerte [<i>Alert service bulletin</i>]
ATC	Contrôle de la circulation aérienne [<i>Air traffic control</i>]
ATM	Gestion du trafic aérien [<i>Air traffic management</i>]
ATS	Service(s) de la circulation aérienne [<i>Air traffic service</i>]
CAN	Avis d'action correctrice [<i>Corrective action notice</i>]
CBA	Analyse coût-avantages [<i>Cost-benefit analysis</i>]
CEO	Directeur général [<i>Chief executive officer</i>]
CFIT	Impact sans perte de contrôle [<i>Controlled flight into terrain</i>]
Cir	Circulaire [<i>Circular</i>]
CM	Surveillance de l'état [<i>Condition monitoring</i>]
CMA	Méthode de surveillance continue [<i>Continuous monitoring approach</i>]
CMC	Centre de gestion des crises [<i>Crisis management centre</i>]
CNS	Communications, navigation et surveillance [<i>Communications, navigation and surveillance</i>]
CP	Poste de commande [<i>Command post</i>]
CRM	Gestion des ressources en équipage [<i>Crew resource management</i>]
CVR	Enregistreur de conversations du poste de pilotage [<i>Cockpit voice recorder</i>]
D&M	Conception et construction [<i>Design and manufacturing</i>]
DGR	Règlement relatif aux marchandises dangereuses [<i>Dangerous goods regulation</i>]
DOA	Agrément d'organisme de conception [<i>Design organization approval</i>]
Doc	Document
EAD	Directive de navigabilité d'urgence [<i>Emergency airworthiness directive</i>]
EC	Maîtrise des risques d'escalade [<i>Escalation control</i>]
ECCAIRS	Centre européen de coordination des systèmes de notification des incidents et accidents d'aviation [<i>European Coordination Centre for Accident and Incident Reporting Systems</i>]
EDTO	Vol à temps de déroutement prolongé [<i>Extended diversion time operation</i>]

EF	Facteur d'escalade (<i>Escalation factor</i>)
EMC	Centre de gestion des urgences (<i>Emergency management centre</i>)
ERP	Plan d'intervention en cas d'urgence (<i>Emergency response plan</i>)
FDR	Enregistreur de données de vol (<i>Flight data recorder</i>)
FH	Heures de vol (<i>Flying hours</i>)
FIR	Région d'information de vol (<i>Flight information region</i>)
FL	Niveau de vol (<i>Flight level</i>)
FTL	Limitation du temps de vol (<i>Flight time limitation</i>)
FTM	Gestion technique de la flotte (<i>Fleet technical management</i>)
GAQ	Questionnaire d'analyse des lacunes (<i>Gap analysis questionnaire</i>)
GRS	Gestion du risque de sécurité (<i>Safety risk management</i>)
GS	Gestion de la sécurité (<i>Safety management</i>)
H	Danger (<i>Hazard</i>)
HF	Facteurs humains (<i>Human factors</i>)
HIRA	Identification des dangers et évaluation des risques (<i>Hazard identification and risk assessment</i>)
HIRM	Identification des dangers et atténuation des risques (<i>Hazard identification and risk mitigation</i>)
IATA	Association du transport aérien International (<i>International Air Transport Association</i>)
IFSD	Arrêt de moteur en vol (<i>In-flight shutdown</i>)
ILS	Système d'atterrissage aux instruments (<i>Instrument landing system</i>)
IMC	Conditions météorologiques de vol aux instruments (<i>Instrument meteorological conditions</i>)
ISO	Organisation internationale de normalisation (<i>International Organization for Standardization</i>)
iSTARS	Système intégré d'analyse et de compte rendu des tendances de la sécurité (<i>Integrated Safety Trend and Reporting System</i>)
ITM	Gestion technique de l'inventaire (<i>Inventory technical management</i>)
kg	Kilogramme(s)
LEI	Manque de mise en œuvre effective (<i>Lack of effective implementation</i>)
LOC-I	Perte de contrôle en vol (<i>Loss of control in flight</i>)
LOFT	Entraînement type vol de ligne (<i>Line oriented flight training</i>)
LOS	Perte de séparation (<i>Loss of separation</i>)
LOSA	Audit de sécurité en service de ligne (<i>Line operations safety audit</i>)
LRU	Unité remplaçable sur place (<i>Line replaceable unit</i>)
LSI	Inspection de station de maintenance en ligne (<i>Line station inspection</i>)
MCM	Manuel de contrôle de maintenance (<i>Maintenance control manual</i>)
MDR	Compte rendu obligatoire de défektivité (<i>Mandatory defect report</i>)
MEDA	Décision sur les erreurs de maintenance (<i>Maintenance error decision aid</i>)
MEL	Liste minimale d'équipements (<i>Minimum equipment list</i>)
MFF	Vols sur plus d'un type ou d'une variante (<i>Mixed fleet flying</i>)
MGS	Manuel de gestion de la sécurité (<i>Safety management manual</i>)
MOR	Compte rendu obligatoire d'événement (<i>Mandatory occurrence report</i>)
MPD	Document de planification de maintenance (<i>Maintenance planning document</i>)
MRM	Gestion des ressources de maintenance (<i>Maintenance resource management</i>)
MRO	Organisme de maintenance/réparation (<i>Maintenance repair organization</i>)
MSL	Niveau moyen de la mer (<i>Mean sea level</i>)

N/A	Sans objet (<i>Not applicable</i>)
OACI	Organisation de l'aviation civile internationale (<i>International Civil Aviation Organization</i>)
OEM	Constructeur de l'équipement d'origine (<i>Original equipment manufacturer</i>)
OPS	Exploitation (<i>Operations</i>)
ORP	Profil de risque de l'organisation (<i>Organization risk profile</i>)
OSC	Culture de sécurité de l'organisation (<i>Organization safety culture</i>)
OSHE	Sécurité professionnelle, santé et environnement (<i>Occupational safety, health and environment</i>)
PC	Contrôle préventif (<i>Preventive control</i>)
PMI	Inspecteur principal de maintenance (<i>Principal maintenance inspector</i>)
PNS	Programme national de sécurité (<i>State safety programme</i>)
POA	Agrément d'organisme de production (<i>Production organization approval</i>)
POI	Inspecteur principal de l'exploitation (<i>Principal operations inspector</i>)
QA	Assurance de la qualité (<i>Quality assurance</i>)
QC	Contrôle de la qualité (<i>Quality control</i>)
QM	Management de la qualité (<i>Quality management</i>)
RAIO	Organisation régionale d'enquête sur les accidents et incidents (<i>Regional accident and incident investigation organization</i>)
RM	Mesure de rétablissement (<i>Recovery measure</i>)
RSOO	Organisation régionale de supervision de la sécurité (<i>Regional safety oversight organization</i>)
SAG	Groupe d'action pour la sécurité (<i>Safety action group</i>)
SARP	Normes et pratiques recommandées (<i>Standards and Recommended Practices</i>)
SB	Bulletin de service (<i>Service bulletin</i>)
SCF-NP	Panne d'une composante du système — autre que le groupe motopropulseur (<i>System component failure — non-powerplant</i>)
SD	Écart standard (<i>Standard deviation</i>)
SDCPS	Système de collecte et de traitement de données sur la sécurité (<i>Safety data collection and processing system</i>)
SGD	Système de gestion des documents [<i>Document management system (DMS)</i>]
SGE	Système de gestion de l'environnement [<i>Environmental management system (EMS)</i>]
SGF	Système de gestion financière [<i>Financial management system (FMS)</i>]
SGQ	Système de gestion de la qualité [<i>Quality management system (QMS)</i>]
SGRF	Systèmes de gestion du risque de fatigue [<i>Fatigue risk management systems (FRMS)</i>]
SGS	Système(s) de gestion de la sécurité [<i>Safety management system(s) (SMS)</i>]
SGSST	Système de gestion de la santé et de la sécurité au travail [<i>Occupational health and safety management system (OHSMS)</i>]
SGSûr	Système de gestion de la sûreté [<i>Security management system (SeMS)</i>]
SHEL	Documents/Matériel/Environnement/Être humain (<i>Software/Hardware/Environment/Liveware</i>)
SMP	Groupe d'experts en gestion de la sécurité (<i>Safety Management Panel</i>)
SOP	Procédure(s) d'exploitation normalisée(s) (<i>Standard operating procedures</i>)
SPI	Indicateur de performance de sécurité (<i>Safety performance indicator</i>)
SRB	Commission d'examen de la sécurité (<i>Safety review board</i>)
SRC	Comité d'examen de la sécurité (<i>Safety review committee</i>)
SSO	Bureau des services de sécurité (<i>Safety services office</i>)
STDEVp	Écart standard de la population (<i>Population standard deviation</i>)

TBD	À déterminer (<i>To be determined</i>)
TOR	Mandat (<i>Terms of reference</i>)
UC	Conséquence ultime (<i>Ultimate consequence</i>)
UE	Événement dangereux (<i>Unsafe event</i>)
USOAP	Programme universel (OACI) d'audits de supervision de la sécurité [<i>Universal Safety Oversight Audit Programme (ICAO)</i>]
WIP	Travaux en cours (<i>Work in progress</i>)

DÉFINITIONS

Note.— Les définitions qui suivent ont été rédigées alors que la nouvelle Annexe 19 — Gestion de la sécurité était en cours d'élaboration. S'il y a des différences entre définitions lorsque l'Annexe 19 deviendra applicable, en novembre 2013, celles de l'Annexe 19 prévaudront.

Atténuation des risques. Processus d'intégration de défenses ou de contrôles préventifs pour réduire la gravité et/ou la probabilité de la conséquence prévue d'un danger.

Défenses. Mesures d'atténuation spécifiques, contrôles préventifs ou mesures de rétablissement mises en place pour empêcher qu'un danger se réalise ou s'accroisse jusqu'à une conséquence indésirable.

Dirigeant responsable (*accountable executive*). Personne identifiable à qui incombe la responsabilité de performances efficaces et efficientes du PNS de l'État ou du SGS du prestataire de services.

Erreurs. Action ou inaction d'une personne en fonction, conduisant à des écarts par rapport aux intentions ou aux attentes de l'organisation ou de cette personne.

Gestion du changement. Processus formel pour gérer systématiquement les changements au sein d'une organisation, afin qu'il soit tenu compte avant leur mise en œuvre des incidences qu'ils pourraient avoir sur les dangers identifiés et sur les stratégies d'atténuation des risques.

Indicateurs de conséquences importantes. Indicateurs de performances de sécurité se rapportant à la surveillance et à la mesure d'événements aux conséquences importantes, tels que des accidents ou des incidents graves. Les indicateurs de conséquences importantes sont parfois appelés indicateurs réactifs.

Indicateurs de moindres conséquences. Indicateurs de performances de sécurité se rapportant à la surveillance et à la mesure de faits, d'événements ou d'activités à moindres conséquences, tels que des incidents, des constats de non-conformité ou des écarts. Les indicateurs de moindres conséquences sont parfois appelés indicateurs proactifs/prédictifs.

Indicateur de performance de sécurité. Paramètre de sécurité basé sur des données qui est utilisé pour surveiller et évaluer les performances de sécurité.

Niveau acceptable de performances de sécurité (ALoSP). Niveau minimum de performances de sécurité de l'aviation civile dans un État, comme défini dans son programme national de sécurité, ou dans celui d'un prestataire de services, comme défini dans son système de gestion de la sécurité, exprimé en termes d'objectifs de performance de sécurité et d'indicateurs de performance de sécurité.

Performance de sécurité. Réalisation en matière de sécurité d'un État ou d'un prestataire de services, définie par ses objectifs de performance de sécurité et ses indicateurs de performance de sécurité.

Programme national de sécurité. Ensemble intégré de règlements et d'activités visant à améliorer la sécurité.

Risque de sécurité. Probabilité et gravité prévues des conséquences ou des résultats d'un danger.

Système de gestion de la sécurité. Méthode systématique de gestion de la sécurité, incluant les structures organisationnelles, obligations de rendre compte, politiques et procédures nécessaires.

Chapitre 1

PRÉSENTATION GÉNÉRALE DU MANUEL

1.1 GÉNÉRALITÉS

1.1.1 Cette troisième édition du *Manuel de gestion de la sécurité (MGS)* (Doc 9859) de l'OACI remplace dans son entièreté la deuxième édition, publiée en 2009. Elle remplace aussi le *Manuel de prévention des accidents* (Doc 9422) de l'OACI, qui est dépassé.

1.1.2 Ce manuel est destiné à apporter aux États des indications sur l'élaboration et la mise en œuvre d'un programme national de sécurité (PNS), en conformité avec les normes et pratiques recommandées (SARP) de l'Annexe 1 — *Licences du personnel*, de l'Annexe 6 — *Exploitation technique des aéronefs*, de l'Annexe 8 — *Navigabilité des aéronefs*, de l'Annexe 11 — *Services de la circulation aérienne*, de l'Annexe 13 — *Enquêtes sur les accidents et incidents d'aviation* et de l'Annexe 14 — *Aérodromes, Volume I — Conception et exploitation technique des aérodromes*. Il est à noter que des dispositions relatives aux PNS seront intégrées dans l'Annexe 19 — *Gestion de la sécurité*, encore en cours d'élaboration au moment de la publication de cette troisième édition. Ce manuel apporte aussi des éléments indicatifs pour l'établissement par les États de spécifications relatives aux systèmes de gestion de la sécurité (SGS), ainsi que pour l'élaboration et la mise en œuvre de SGS par les fournisseurs de produits et de services concernés.

1.1.3 Il est à noter que ce manuel est destiné à être utilisé conjointement avec d'autres éléments indicatifs appropriés utilisables pour compléter ou renforcer les concepts ou les orientations qu'il contient.

Note.— Dans le contexte de la gestion de la sécurité, le terme « prestataire de services » ou « fournisseur de produits et de services » se rapporte à tout organisme qui fournit des produits et/ou des services d'aviation. Ce terme englobe donc les organismes de formation agréés qui sont exposés à des risques de sécurité pendant la prestation de leurs services, exploitants d'aéronefs, organismes de maintenance agréés, organismes responsables de la conception de type et/ou de la construction des aéronefs, fournisseurs de services de la circulation aérienne et aérodromes certifiés.

1.2 OBJECTIF

L'objectif de ce manuel est d'apporter aux États et aux fournisseurs de produits et de services :

- a) un aperçu général des notions fondamentales de gestion de la sécurité ;
- b) un résumé des SARP de l'OACI relatives à la gestion de la sécurité figurant dans les Annexes 1, 6, 8, 11, 13 et 14 ;
- c) des éléments indicatifs sur la manière d'élaborer et mettre en œuvre un PNS en conformité avec les SARP pertinentes de l'OACI, y compris un cadre réglementaire harmonisé pour la supervision des SGS des fournisseurs de produits et de services ;
- d) des orientations sur l'élaboration, la mise en œuvre et la tenue à jour d'un SGS.

1.3 STRUCTURE

Le Chapitre 1 présente un aperçu général du manuel, tandis que le Chapitre 2 traite des concepts et des processus fondamentaux de gestion de la sécurité. Le Chapitre 3 donne un aperçu des SARP de l'OACI figurant dans les Annexes 1, 6, 8, 11, 13 et 14. Enfin, les Chapitres 4 et 5 exposent une méthode progressive d'élaboration, de mise en œuvre et de tenue à jour d'un PNS et d'un SGS. Ces deux derniers chapitres contiennent aussi des appendices qui apportent des éléments d'orientation pratiques et des illustrations. Le Supplément au manuel contient une liste d'éléments d'orientation connexes de l'OACI.

Note.— Dans ce manuel, le terme « homme » s'entend comme incluant hommes et femmes.

Chapitre 2

NOTIONS FONDAMENTALES DE GESTION DE LA SÉCURITÉ

Note.— Ce chapitre donne un aperçu des concepts et pratiques fondamentaux de gestion de la sécurité qui sont applicables à la mise en œuvre de programmes nationaux de sécurité ainsi qu'à la mise en œuvre et à la supervision de systèmes de gestion de la sécurité par les fournisseurs de produits et de services. Le contenu de ce chapitre est une introduction, de plus amples précisions sur ces questions étant apportées dans les chapitres ultérieurs du manuel.

2.1 LE CONCEPT DE SÉCURITÉ

2.1.1 Dans le contexte de l'aviation, la sécurité est « l'état dans lequel la possibilité de lésions corporelles ou de dommages matériels est réduite à un niveau acceptable, et maintenue à ce niveau ou au-dessous de ce niveau, par un processus continu d'identification des dangers et de gestion des risques de sécurité. »

2.1.2 Même si l'élimination des accidents d'aviation et/ou des incidents graves demeure le but ultime, il est reconnu que l'aviation ne peut être complètement exempte de dangers et des risques connexes. Les activités humaines ou les systèmes construits par l'homme ne peuvent être garantis comme étant entièrement exempts d'erreurs opérationnelles et de leurs conséquences. La sécurité est donc une caractéristique dynamique du système d'aviation, où les risques de sécurité doivent être constamment atténués. Il est à noter que l'acceptabilité des performances de sécurité est souvent influencée par les normes nationales ou internationales et par la culture. Tant que les risques de sécurité sont maintenus sous un niveau approprié de contrôle, un système aussi ouvert et dynamique que l'est l'aviation peut encore être géré de manière à maintenir l'équilibre approprié entre production et protection.

2.2 L'ÉVOLUTION DE LA SÉCURITÉ

L'histoire des avancées en matière de sécurité de l'aviation peut être divisée en trois époques :

- a) *L'époque technique — du début des années 1900 à la fin des années 1960.* L'aviation a vu le jour comme une forme de transport de masse dans laquelle les carences de sécurité identifiées ont été initialement reliées à des facteurs techniques et à des défaillances technologiques. Les efforts pour la sécurité se sont donc focalisés sur les investigations et sur l'amélioration de facteurs techniques. Dès les années 1950, les améliorations technologiques ayant mené à une réduction progressive de la fréquence des accidents, les processus de sécurité ont été élargis pour englober la conformité à la réglementation et la supervision.
- b) *L'époque des facteurs humains — du début des années 1970 au milieu des années 1990.* Au début des années 1970, la fréquence des accidents d'aviation a été nettement réduite grâce à des avancées technologiques majeures et à des améliorations de la réglementation en matière de sécurité. L'aviation est devenue un mode de transport plus sûr, et la focalisation des activités de sécurité s'est étendue aux questions de facteurs humains, y compris l'interface homme/machine. Ceci a mené à des recherches de renseignements sur la sécurité au-delà de ceux qui étaient issus du processus antérieur d'enquêtes sur les accidents. Malgré l'investissement de ressources dans l'atténuation des erreurs, la performance

humaine continuait d'être citée comme facteur récurrent d'accidents (Figure 2-1). L'application de la science des facteurs humains avait tendance à se focaliser sur l'individu, sans prendre entièrement en considération le contexte opérationnel et organisationnel. Ce n'est pas avant le début des années 1990 qu'il a commencé à être reconnu que les individus opèrent dans un environnement complexe, qui inclut de multiples facteurs ayant le potentiel d'affecter le comportement.

- c) *L'époque organisationnelle — du milieu des années 1990 à nos jours.* À l'époque organisationnelle, la sécurité a commencé à être considérée dans une perspective systémique, consistant à englober les facteurs organisationnels en plus des facteurs humains et techniques. Il en est résulté l'introduction de la notion d'« accident organisationnel », prenant en considération l'impact de la culture et des politiques organisationnelles sur l'efficacité de la maîtrise des risques de sécurité. De plus, les activités traditionnelles de collecte et d'analyse de données, limitées à l'utilisation de données recueillies lors des enquêtes sur les accidents et les incidents graves, ont été complétées par une nouvelle approche proactive de la sécurité. Cette nouvelle approche se fonde sur la collecte et l'analyse régulières de données employant des méthodes tant proactives que réactives pour surveiller les risques de sécurité connus et détecter les problèmes de sécurité émergents. Ces améliorations ont établi la logique de l'évolution vers une méthode de gestion de la sécurité.

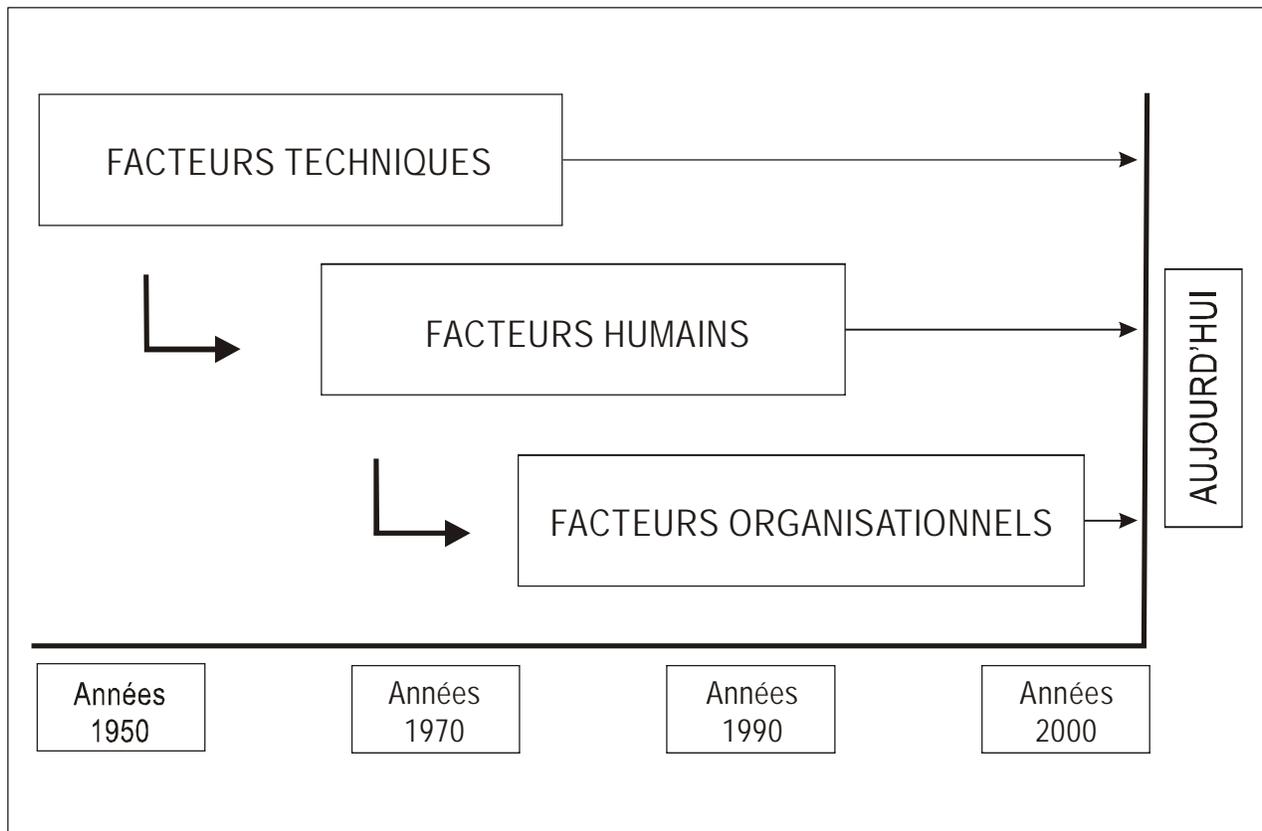


Figure 2-1. L'évolution de la sécurité

2.3 CAUSALITÉ DES ACCIDENTS

2.3.1 Le modèle du « fromage suisse », proposé par le professeur James Reason, montre que les accidents font intervenir des ruptures successives de multiples défenses du système. Ces ruptures peuvent être déclenchées par plusieurs facteurs tels que des défaillances de l'équipement ou des erreurs opérationnelles. Selon le modèle de Reason, des systèmes aussi complexes que l'aviation étant extrêmement bien défendus par des couches de défenses, il est rare, dans de tels systèmes, que des défaillances en un point unique portent à conséquence. Des ruptures des défenses de sécurité peuvent être une conséquence retardée de décisions prises aux plus hauts niveaux du système, pouvant rester en sommeil jusqu'à ce que leurs effets ou leur potentiel dommageable soient activés par certaines circonstances opérationnelles. Dans de telles circonstances particulières, des défaillances humaines ou des défaillances actives au niveau opérationnel agissent pour rompre les défenses de sécurité intrinsèques du système. Selon le modèle de Reason, tous les accidents comprennent une combinaison de conditions actives et de conditions latentes.

2.3.2 Les défaillances actives sont des actions ou des inactions, incluant erreurs et violations, qui ont un effet adverse immédiat. Elles sont généralement considérées, rétrospectivement, comme des actes dangereux. Les défaillances actives sont généralement associées au personnel de première ligne (pilotes, contrôleurs de la circulation aérienne, mécaniciens d'aéronefs, etc.) et peuvent entraîner des résultats dommageables.

2.3.3 Les conditions latentes sont des conditions présentes dans le système d'aviation bien avant que se produise un résultat dommageable. Leurs conséquences peuvent rester longtemps en dormance. Initialement, ces conditions latentes ne sont pas perçues comme dommageables, mais elles deviendront évidentes une fois que les défenses du système auront été rompues. Ces conditions sont généralement créées par des personnes éloignées de l'événement dans le temps et l'espace. Les conditions latentes dans le système peuvent inclure des conditions créées par un manque de culture de sécurité, par un équipement médiocre ou une mauvaise conception des procédures, par des objectifs organisationnels conflictuels ou par des défauts dans les systèmes d'organisation ou les décisions managériales. La perspective sous-jacente au concept d'accident organisationnel vise à identifier et atténuer ces conditions latentes sur une base systémique, plutôt que par des efforts localisés pour réduire les défaillances actives d'individus.

2.3.4 La Figure 2-2 montre comment le modèle du « fromage suisse » aide à comprendre les interactions de facteurs organisationnels et managériaux dans la causalité des accidents. Il montre que diverses défenses sont intégrées dans le système d'aviation pour assurer une protection contre les fluctuations dans la performance ou les décisions humaines à tous les niveaux du système. Ces défenses agissent pour protéger contre les risques de sécurité, mais des ruptures pénétrant toutes les barrières défensives pourraient avoir pour résultat une situation catastrophique. Le modèle de Reason montre, en outre, comment des conditions latentes présentes au sein du système avant l'accident peuvent se manifester du fait de facteurs déclencheurs locaux.

L'accident organisationnel

2.3.5 C'est par une approche modulaire, à cinq modules (Figure 2-3), que la notion d'accident organisationnel, qui sous-tend le modèle de Reason, peut être le mieux comprise. Le module du haut représente les processus organisationnels. Ce sont des activités sur lesquelles toute organisation a un degré raisonnable de contrôle direct. Des exemples types sont : l'établissement des politiques, la planification, la communication, l'attribution de ressources et la supervision. Les deux processus organisationnels fondamentaux en ce qui concerne la sécurité sont indubitablement l'attribution de ressources et la communication. Des faiblesses ou des carences dans ces processus organisationnels sont le terrain propice pour un double parcours vers une défaillance.

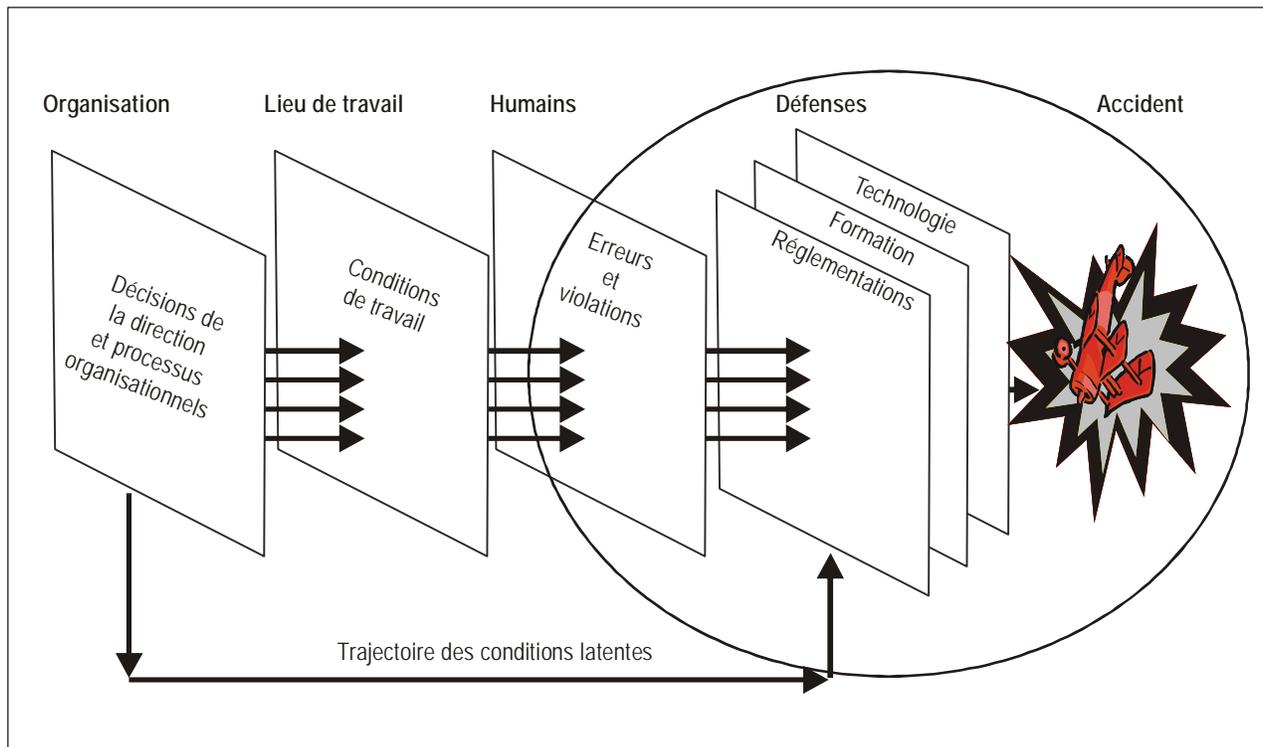


Figure 2-2. Concept de causalité de l'accident

2.3.6 L'un de ces parcours est celui des conditions latentes. Des exemples de conditions latentes sont notamment : carences dans la conception de l'équipement, procédures d'exploitation normalisées incomplètes/défectueuses, carences de la formation. En termes génériques, les conditions latentes peuvent être groupées en deux grandes grappes. Les insuffisances dans l'identification des dangers et la gestion des risques constituent la première grappe : les risques de sécurité découlant des conséquences de dangers ne sont pas maîtrisés, mais évoluent librement dans le système pour être finalement activés par des déclencheurs opérationnels.

2.3.7 La seconde grappe recouvre ce que l'on appelle une normalisation de la déviance, notion qui, pour le dire simplement, s'applique à des contextes opérationnels où l'exception devient la règle. L'affectation de ressources est, dans ce cas, déficiente à l'extrême. Faute de ressources, la seule façon de réaliser ces activités avec succès est, pour le personnel opérationnel chargé de la réalisation concrète des activités de production, d'adopter des raccourcis impliquant une violation constante des règles et des procédures.

2.3.8 Les conditions latentes ont toutes le potentiel de rompre les défenses du système d'aviation. De façon générale, en aviation, les défenses peuvent être groupées sous trois grands titres : technologie, formation et règlements. Elles sont habituellement le dernier filet de sécurité pour circonscrire les conditions latentes, ainsi que les conséquences de défaillances dans la performance humaine. La plupart des stratégies d'atténuation des risques de sécurité découlant des conséquences de dangers, sinon toutes, se fondent sur le renforcement de défenses existantes ou le développement de défenses nouvelles.

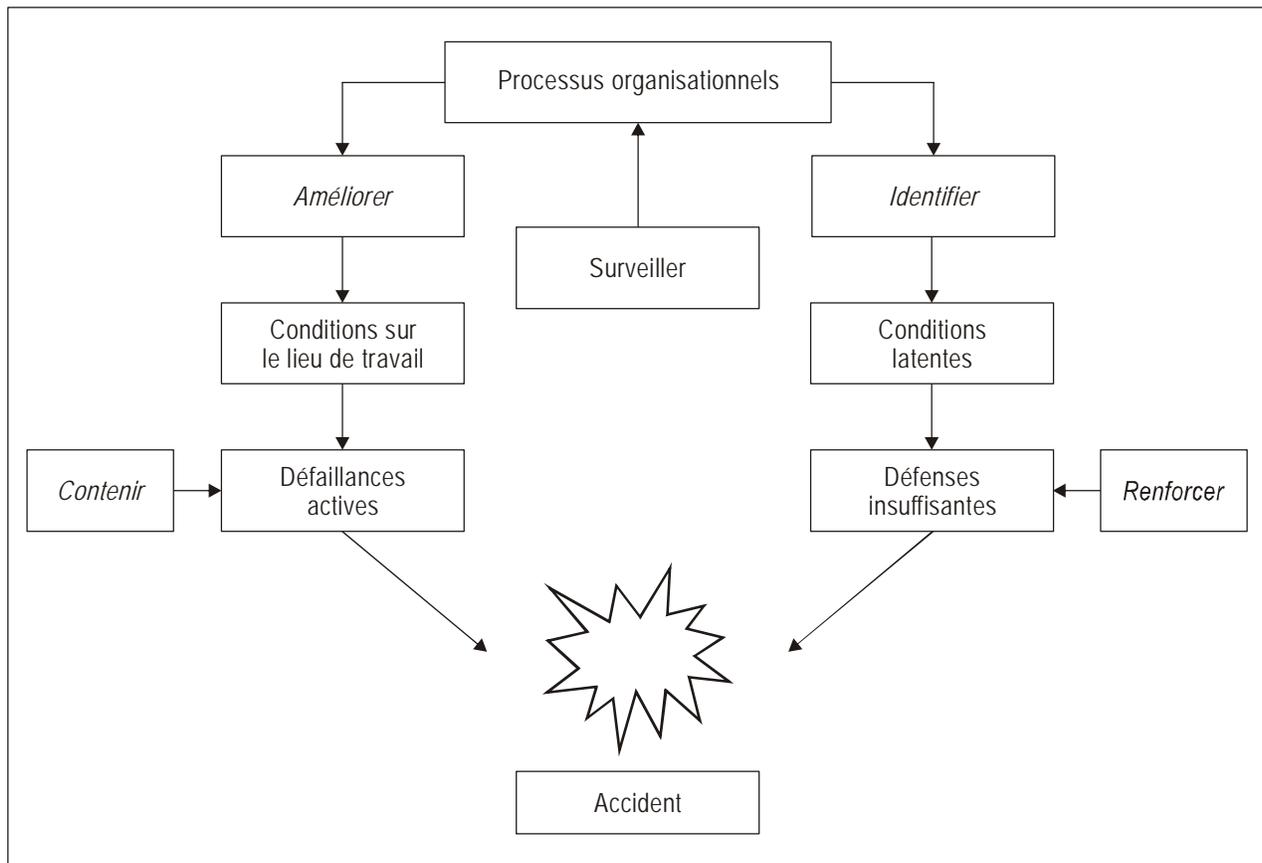


Figure 2-3 L'accident organisationnel

2.3.9 L'autre parcours ayant son origine dans les processus organisationnels est celui des conditions sur le lieu de travail. Il s'agit là de facteurs qui influencent directement l'efficacité des personnes sur les lieux de travail de l'aviation. Les conditions sur le lieu de travail sont largement intuitives, en ce sens que tous ceux qui ont une expérience opérationnelle en ont l'expérience à divers degrés ; elles comprennent : la stabilité du personnel, ses qualifications et son expérience, la crédibilité du management, et des facteurs ergonomiques traditionnels tels que l'éclairage, le chauffage et la climatisation.

2.3.10 Des conditions sous-optimales sur le lieu de travail suscitent des défaillances actives du personnel opérationnel. Les défaillances actives peuvent être considérées soit comme des erreurs, soit comme des violations. La différence entre erreurs et violations est l'élément d'intentionnalité. Une personne qui s'efforce d'accomplir une tâche le mieux possible, en suivant les règles et les procédures conformément à la formation qu'elle a reçue, mais sans parvenir à atteindre son objectif, commet une erreur. Une personne qui, en accomplissant une tâche, s'écarte volontairement des règles, des procédures et de la formation reçue commet une violation. C'est donc l'intention qui constitue la différence fondamentale entre erreurs et violations.

2.3.11 Dans la perspective de l'accident organisationnel, les efforts pour la sécurité devraient porter sur la surveillance des processus organisationnels afin d'identifier les conditions latentes et de renforcer ainsi les défenses. Les efforts pour la sécurité devraient aussi améliorer les conditions sur le lieu de travail afin de circonscrire les défaillances actives, car c'est l'enchaînement de tous ces facteurs qui produit des défaillances de la sécurité.

La dérive pratique

2.3.12 Sur la base de la théorie de la dérive pratique, de Scott A. Snook, on pourra comprendre comment, en aviation, la performance de référence de n'importe quel système « dérive » de sa conception d'origine lorsque les processus et procédures de l'organisation ne peuvent anticiper toutes les situations susceptibles de se produire dans les opérations quotidiennes.

2.3.13 Aux premiers stades de la conception du système (p. ex. espace aérien ATC, introduction de certains équipements, expansion d'un modèle d'opérations aériennes), les interactions opérationnelles entre les humains et la technologie, ainsi que le contexte opérationnel, sont pris en considération pour identifier les limitations de performances à prévoir ainsi que les dangers potentiels. Le système initial est basé sur trois hypothèses fondamentales : la technologie nécessaire pour atteindre les objectifs de production du système est disponible, les gens sont formés pour bien utiliser la technologie, et les règlements et procédures dicteront le comportement du système et des humains. Ces hypothèses sous-tendent la performance de référence (ou idéale) du système, qui peut être présentée sous forme graphique comme une ligne droite allant de la date du déploiement opérationnel du système jusqu'à son retrait du service (Figure 2-4).

2.3.14 Une fois déployé de façon opérationnelle, le système fonctionne comme il a été conçu, la plupart du temps selon la performance de référence. En réalité, cependant, la performance opérationnelle est différente de la performance de référence en conséquence des opérations dans la vie réelle et de changements dans le contexte opérationnel et réglementaire. La dérive étant une conséquence de la pratique quotidienne, elle est appelée « dérive pratique ». Le terme « dérive » est employé dans ce contexte pour désigner l'écart progressif, du fait d'influences extérieures, par rapport à un parcours prévu.

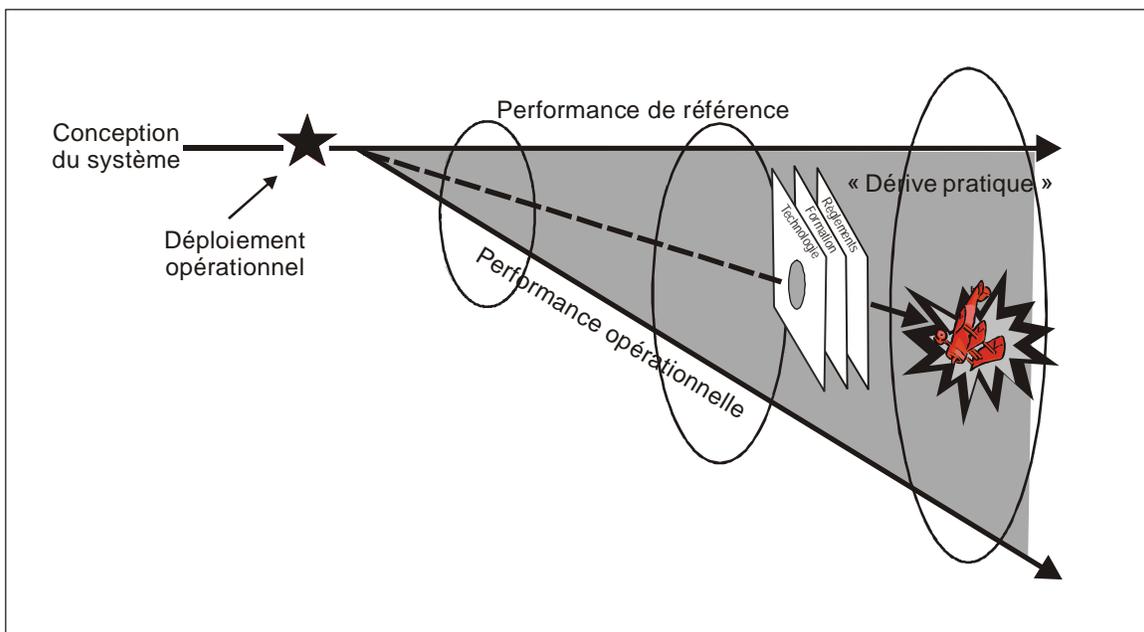


Figure 2-4. La dérive pratique

2.3.15 Une dérive pratique de la performance de référence vers la performance opérationnelle est prévisible dans n'importe quel système, aussi soignée et bien pensée qu'ait pu être sa planification conceptuelle. Certaines des raisons de la dérive pratique peuvent être : une technologie ne fonctionnant pas toujours comme prévu ; des procédures qui, dans certaines circonstances opérationnelles, ne peuvent pas être exécutées comme cela a été planifié ; des règlements qui ne sont pas applicables dans certaines limites contextuelles ; l'introduction de changements dans le système, notamment l'addition de nouveaux éléments ; l'interaction avec d'autres systèmes, etc. Le fait demeure cependant que, en dépit de toutes les insuffisances du système menant à une dérive, les humains opérant au sein de la dérive pratique font fonctionner le système quotidiennement, en appliquant des adaptations locales (ou contournements) et des stratégies personnelles « au-delà de ce que dit le livre ».

2.3.16 Comme l'explique la Figure 2-4, saisir et analyser les renseignements sur ce qui se produit au sein de la dérive pratique comporte un potentiel considérable d'apprentissage sur des adaptations de sécurité réussies et, donc, pour le contrôle et l'atténuation des risques de sécurité. Plus les renseignements peuvent être systématiquement saisis près du commencement de la dérive pratique, et plus grand sera le nombre de dangers et de risques de sécurité qui pourront être prédits et dont on pourra s'occuper, ce qui mènera à des interventions formelles pour revoir la conception du système ou lui apporter des améliorations. Cependant, la prolifération incontrôlée d'adaptations locales et de stratégies personnelles pourrait mener à ce que la dérive pratique s'écarte trop de la performance de référence attendue, à tel point qu'un incident ou un accident devienne une plus grande possibilité.

2.4 HUMAINS, CONTEXTE ET SÉCURITÉ

2.4.1 Le système de l'aviation inclut les producteurs de produits et services et les organismes de l'État. C'est un système complexe qui exige d'évaluer la contribution humaine à la sécurité et de comprendre comment la performance humaine peut être affectée par ses multiples composantes interdépendantes.

2.4.2 Le modèle SHELL est un outil conceptuel pour analyser l'interaction des composantes multiples d'un système. La Figure 2-5 donne une description de base de la relation entre les humains et les autres composantes du lieu de travail. Le nom de ce modèle est constitué des initiales de ses quatre composantes :

- a) *Software (S)* : procédures, formation, soutien, etc. ;
- b) *Hardware (H)* : machines et équipement ;
- c) *Environnement (E)* : environnement de travail dans lequel le reste du système L-H-S doit fonctionner ;
- d) *Liveware (L)* : humains sur le lieu de travail.

2.4.3 *Liveware*. Au centre du modèle SHELL se trouvent les humains, en première ligne des opérations. Malgré leurs remarquables facultés d'adaptation, les humains sont sujets à de considérables variations de performance. Ils ne sont pas standardisés comme l'est le matériel, ce qui explique pourquoi les bords de ce cube ne sont pas simples et rectilignes. Les interfaces entre les humains et les diverses composantes du monde où ils travaillent ne sont pas parfaites. Pour éviter les tensions qui pourraient compromettre la performance humaine, il faut comprendre les effets des irrégularités aux interfaces entre les différents cubes du modèle SHELL et le cube central *Liveware*. Si l'on veut éviter des tensions dans le système, il faut faire correspondre soigneusement les autres composantes du système avec les humains. Le modèle SHELL est utile pour visualiser les interfaces suivantes entre les divers éléments du système d'aviation :

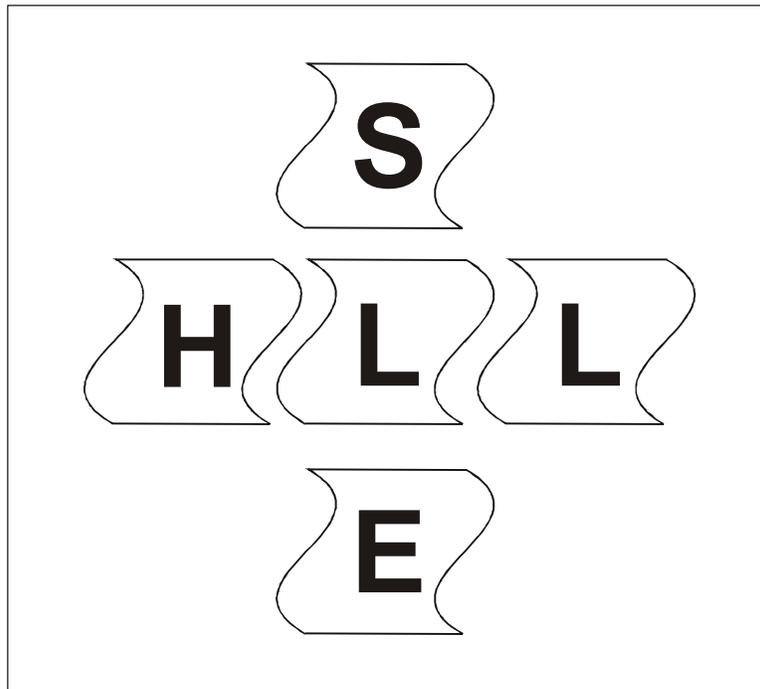


Figure 2-5. Le modèle SHELL — composantes et interfaces

- a) *Liveware-Hardware (L-H)*. L'interface L-H représente les relations entre l'humain et les attributs physiques de l'équipement, des machines et des installations. L'interface entre l'humain et la technologie est celle qui est le plus souvent envisagée lorsque l'on parle de performance humaine dans le contexte des opérations d'aviation, et il existe une tendance humaine naturelle à s'adapter à des décalages entre L et H. Cette tendance peut masquer des carences graves qui n'apparaîtront qu'après un événement.
- b) *Liveware-Software (L-S)*. L'interface L-S est la relation entre l'humain et les systèmes de support qui se trouvent sur le lieu de travail, tels que règlements, manuels, listes de vérification, publications, SOP et logiciels. Cette interface inclut des questions telles que récence de l'expérience, précision, forme et présentation, vocabulaire, clarté et symbologie.
- c) *Liveware-Liveware (L-L)*. L'interface L-L représente les relations interpersonnelles sur le lieu de travail. Équipes de conduite, contrôleurs de la circulation aérienne, mécaniciens d'entretien d'aéronef et autres membres du personnel opérationnel ont un fonctionnement de groupe, et il importe de reconnaître que les compétences de communication et interpersonnelles, ainsi que la dynamique de groupe, jouent un rôle déterminant dans les performances humaines. L'apparition de la gestion des ressources en équipage (CRM) et son extension aux services de la circulation aérienne (ATS) et à la maintenance ont focalisé l'attention sur la gestion des erreurs opérationnelles dans les multiples domaines de l'aviation. Les relations entre le personnel et l'encadrement se situent également à cette interface, de même que la culture organisationnelle dans son ensemble.
- d) *Liveware-Environment (L-E)*. Cette interface concerne les relations entre l'être humain et les environnements intérieur et extérieur. L'environnement intérieur du lieu de travail comprend des considérations physiques telles que température, lumière ambiante, bruit, vibrations et qualité de l'air.

L'environnement extérieur comprend des aspects opérationnels tels que facteurs météorologiques, infrastructure aéronautique et relief. Cette interface fait intervenir aussi la relation entre l'environnement intérieur de l'humain et son environnement extérieur. Des forces psychologiques et physiologiques, notamment la maladie, la fatigue, les incertitudes financières, et les préoccupations de relations et de carrière, peuvent être induites par les interactions L-E ou avoir leur origine dans des sources extérieures secondaires. L'environnement de travail de l'aviation inclut des perturbations des rythmes biologiques normaux et des cycles du sommeil. D'autres aspects environnementaux peuvent être en rapport avec des attributs organisationnels qui peuvent affecter les processus de prise de décision et créer des pressions pour développer des « contournements » (*workarounds*) ou écarts mineurs par rapport aux procédures de fonctionnement normales.

2.4.4 D'après le modèle SHELL, un défaut de concordance entre l'élément *Liveware* et les quatre autres éléments contribue à l'erreur humaine. Il faut donc que ces interactions soient évaluées et considérées dans tous les secteurs du système d'aviation.

2.5 ERREURS ET VIOLATIONS

2.5.1 Une mise en œuvre efficace du SGS par le fournisseur de produits ou de services ainsi qu'une supervision effective du SGS par l'État dépendent d'une compréhension claire, des deux côtés, des erreurs et des violations ainsi que de la différenciation entre les deux. La différence entre erreurs et violations réside dans l'intention. Alors que l'erreur n'est pas intentionnelle, une violation est un acte délibéré de conduite fautive ou une omission délibérée pour s'écarter des procédures, protocoles, normes ou pratiques établis.

2.5.2 Erreurs ou violations peuvent avoir pour résultat une non-conformité aux règlements ou aux procédures d'exploitation approuvées. Des mesures punitives prises en réponse à des actes de non-conformité peuvent conduire à une réduction dans les comptes rendus d'erreurs en l'absence d'autres processus. L'État et le fournisseur de produits ou de services doivent donc considérer si les actes de non-conformité sont le résultat d'une violation ou d'une erreur par inadvertance lorsqu'il s'agit de déterminer si des mesures punitives s'imposent, le critère consistant normalement à déterminer si la non-conformité résulte d'une faute intentionnelle ou d'une négligence grave.

Erreurs

2.5.3 Comme indiqué précédemment, une erreur est définie comme « action ou inaction d'une personne en fonction, qui conduit à des écarts par rapport aux intentions ou aux attentes de l'organisation ou de cette personne ». Dans le contexte d'un SGS, aussi bien l'État que le fournisseur de produits ou de services doivent comprendre que, et s'attendre à ce que, les humains commettent des erreurs indépendamment du niveau de technologie utilisé, du niveau de formation ou de l'existence de règlements, processus et procédures. Un objectif important est alors d'établir et de maintenir des défenses pour réduire la probabilité d'erreurs et, ce qui est tout aussi important, de réduire les conséquences des erreurs qui se produisent. Pour que cette tâche puisse être accomplie efficacement, il faut que les erreurs soient identifiées, qu'il en soit rendu compte et qu'elles soient analysées afin que des mesures correctives puissent être prises. Les erreurs peuvent être réparties en deux catégories, comme suit :

- a) À propos des défaillances dans l'exécution de l'action voulue, l'anglais emploie les termes *slips* (glissements), pour des actions qui ne se déroulent pas comme prévu (par exemple, actionner le levier de commande du volet au lieu de celui du train, comme on voulait le faire), et *lapses* (oublis) pour des défaillances de la mémoire (par exemple, oublier un élément d'une liste de vérification).
- b) Le terme *mistake* est appliqué à des défauts dans le plan d'action. Même si l'exécution du plan était correcte, il n'aurait pas été possible de réaliser le résultat voulu.

2.5.4 Des stratégies de sécurité doivent être mises en place pour maîtriser les erreurs ou les éliminer. Les stratégies de maîtrise des erreurs font appel aux défenses de base dans le système d'aviation. Il s'agit de :

- a) *Stratégies de réduction*, prévoyant une intervention directe pour réduire ou éliminer les facteurs qui contribuent à l'erreur. Des exemples de stratégies de réduction comprennent l'amélioration des facteurs ergonomiques et la réduction des distractions liées à l'environnement.
- b) *Stratégies de capture*, supposant que l'erreur sera commise. L'intention est de « capter » l'erreur avant que ses conséquences soient ressenties. Les stratégies de capture sont différentes des stratégies de réduction en ce qu'elles utilisent des listes de vérification et d'autres interventions fondées sur des procédures, plutôt que d'éliminer directement l'erreur.
- c) *Stratégies de tolérance*, faisant appel à la capacité d'un système d'accepter qu'une erreur soit faite, mais sans qu'elle ait des conséquences graves. L'intégration de systèmes redondants ou de processus d'inspection multiples sont des exemples de mesures qui accroissent la tolérance du système à des erreurs.

2.5.5 La performance du personnel étant généralement influencée par des facteurs organisationnels, réglementaires et environnementaux, la gestion des risques de sécurité doit inclure la considération de politiques, processus et procédures opérationnels se rapportant aux communications, aux horaires du personnel, à l'affectation de ressources et aux contraintes budgétaires qui peuvent contribuer à l'incidence d'erreurs.

Violations

2.5.6 Une violation est définie comme « un acte délibéré de conduite fautive ou d'omission ayant pour résultat un écart par rapport aux règlements, procédures, normes ou pratiques établis ». Néanmoins, la non-conformité n'est pas nécessairement le résultat d'une violation, car des écarts par rapport aux exigences réglementaires ou aux procédures d'exploitation peuvent être le résultat d'une erreur. Pour compliquer encore le problème, les violations sont des actes intentionnels, mais ce ne sont pas toujours des actes répondant à une intention malveillante. Des personnes peuvent s'écarter des normes délibérément, dans la conviction que la violation facilitera la réalisation de leur mission sans créer de conséquences défavorables. Des violations de cette nature sont des erreurs de jugement et, en fonction des politiques en place, elles n'aboutiront peut-être pas automatiquement à des mesures disciplinaires. Les violations de ce type peuvent être réparties en catégories, comme suit :

- a) *Violations situationnelles*, commises en réaction à des facteurs rencontrés dans un contexte particulier, tel que des contraintes de temps ou une forte charge de travail.
- b) *Violations de routine*, qui deviennent la façon d'agir normale au sein d'un groupe de travail. De telles violations sont commises en réponse à des situations dans lesquelles la conformité aux procédures établies rend difficile la réalisation de la tâche. Cela peut être dû à des problèmes de considérations pratiques/d'applicabilité, de carences dans la conception de l'interface humain-technologie et d'autres problèmes amenant des personnes à adopter des procédures de « contournement », qui deviennent finalement de la routine. Ces écarts, à propos desquels on parle de « dérive », peuvent se poursuivre sans conséquences, mais, avec le temps, ils peuvent devenir fréquents et entraîner des conséquences qui peuvent être graves. Dans certains cas, les violations de routine sont bien fondées et peuvent mener à l'intégration de la violation de routine comme procédure admise après qu'une évaluation de sécurité en bonne et due forme aura été effectuée et aura montré que la sécurité n'est pas compromise.
- c) *Violations induites par l'organisation*, pouvant être considérées comme extension des violations de routine. Ce type de violation a tendance à se produire lorsqu'une organisation tente de répondre à des exigences de rendement accru en ignorant ses défenses de sécurité ou en les étirant.

2.6 CULTURE DE SÉCURITÉ

2.6.1 La culture est caractérisée par les croyances, les valeurs, les préjugés/partis pris et le comportement qui en résulte, que partagent les membres d'une société, d'un groupe ou d'une organisation. Une compréhension de ces éléments culturels, et des interactions entre eux, est importante pour la gestion de la sécurité. Les trois éléments culturels les plus influents sont les cultures organisationnelles, professionnelles et nationales. Une culture de compte rendu est un élément clé de ces différentes cultures. Le mélange d'éléments culturels peut varier grandement entre organisations et peut influencer négativement le compte rendu de dangers, l'analyse collaborative des causes profondes et l'atténuation des risques acceptables. Une amélioration continue dans les performances en matière de sécurité est possible lorsque la sécurité devient une valeur au sein de l'organisation aussi bien qu'une priorité au niveau national ou professionnel.

2.6.2 Une culture de sécurité englobe les perceptions et convictions qu'ont généralement les membres d'une organisation vis-à-vis de la sécurité publique et elle peut être un élément déterminant de leur comportement. Une saine culture de sécurité repose sur un haut niveau de confiance et de respect entre le personnel et la direction, et doit donc être créée et soutenue au niveau de la haute direction.

2.6.3 Un saine culture de sécurité recherche des améliorations, reste vigilante et consciente des dangers et utilise des systèmes et des outils pour la surveillance continue, l'analyse et les investigations. Elle doit exister aussi bien au niveau des organismes d'aviation nationaux qu'au niveau des organismes fournisseurs de produits et de services. D'autres caractéristiques d'une saine culture de sécurité sont l'engagement partagé du personnel et de la direction vis-à-vis des responsabilités personnelles en matière de sécurité, la confiance dans le système de sécurité et un ensemble de règles et de politiques bien documentées. C'est au niveau du management de l'organisation que se situe la responsabilité ultime de l'établissement et du respect de saines pratiques de sécurité. Une culture de sécurité ne peut être efficace que si elle est ancrée dans la culture d'une organisation elle-même.

2.6.4 La notion de *culture organisationnelle* fait référence aux caractéristiques et aux perceptions de la sécurité entre membres qui interagissent au sein d'une certaine entité. Les systèmes de valeur des organisations incluent les politiques de priorisation ou de réalisation d'un équilibre dans des domaines tels que productivité vs. qualité, sécurité vs. efficacité, financier vs. technique, professionnel vs. académique, et application vs. mesures correctives.

2.6.5 C'est au niveau organisationnel que se trouve le plus grand potentiel de création et de maintien d'une culture efficace, qui s'auto-entretient, pour la gestion de la sécurité. L'organisation est un élément déterminant majeur du comportement, dans lequel des personnes s'engageront en exerçant des activités de gestion ou opérationnelles pendant la réalisation ou la supervision d'activités d'aviation. La culture de l'organisation fixe les limites de la performance de direction et opérationnelle acceptée en établissant les normes et les limites. La culture organisationnelle est donc une pierre angulaire, pour la prise de décision au niveau des dirigeants aussi bien que des employés.

2.6.6 La culture organisationnelle a le potentiel d'influer sur :

- a) les interactions entre membres *senior* et *junior* d'un groupe ;
- b) les interactions entre personnel de l'industrie et personnel de l'autorité de réglementation ;
- c) le degré de partage des informations à l'interne et avec les autorités de réglementation ;
- d) l'existence d'un esprit d'équipe au sein de l'autorité de réglementation ou de l'organisme de l'industrie ;
- e) les réactions du personnel dans des conditions opérationnelles exigeantes ;
- f) l'acceptation et l'utilisation de technologies particulières ;

- g) la tendance à prendre des mesures punitives en réaction à des erreurs opérationnelles chez un fournisseur de produits ou de services ou de la part d'autorités de réglementation.

2.6.7 La culture organisationnelle est influencée aussi par des facteurs tels que :

- a) politiques et procédures d'entreprise ;
- b) comportement et pratiques de supervision ;
- c) objectifs d'amélioration de la sécurité ainsi que niveaux de tolérance minimaux ;
- d) attitude de la direction vis-à-vis des problèmes de qualité ou de sécurité ;
- e) formation et motivation des employés ;
- f) relation entre autorités de réglementation et fournisseurs de produits et services ;
- g) politiques en matière d'équilibre entre travail et vie personnelle.

2.6.8 La manière dont le management traite des questions quotidiennes de sécurité est également fondamentale pour améliorer la culture organisationnelle. Des interactions collaboratives entre le personnel de première ligne et ses homologues de la sécurité et de la qualité, ainsi que les représentants de l'autorité de réglementation, sont indicatives d'une culture organisationnelle positive. Cette relation devrait être caractérisée par la courtoisie professionnelle, tout en maintenant les rôles respectifs comme il est nécessaire pour assurer l'objectivité ou l'obligation de rendre compte.

2.6.9 Une manière efficace de promouvoir la sécurité des opérations est de veiller à ce qu'une organisation ait développé un environnement où tout le personnel se sent responsable pour la sécurité. Ceci devient évident lorsque le personnel considère les incidences sur la sécurité dans tout ce qu'il fait, rend compte de tous les dangers, erreurs et menaces et appuie l'identification et la gestion de tous les risques connexes. De plus, le management doit créer un environnement où le personnel est averti de tous les risques de sécurité, est pourvu de systèmes adéquats pour se protéger et est assuré d'une protection lorsqu'il divulgue des informations relatives à la sécurité par le système de compte rendu de sécurité. Une culture de sécurité efficace sert de méthode pour synchroniser diverses cultures nationales et professionnelles dans le contexte de l'organisation.

2.6.10 La *culture professionnelle* différencie les caractéristiques de groupes professionnels particuliers (c'est-à-dire le comportement caractéristique des pilotes vis-à-vis de celui des contrôleurs de la circulation aérienne, du personnel de l'autorité de l'aviation civile ou des ingénieurs de maintenance). À travers la sélection du personnel, l'éducation, la formation, l'expérience professionnelle ou la pression des pairs, les professionnels ont tendance à adopter le système de valeurs et à développer des modèles de comportement en cohérence avec ceux de leurs pairs ou de leurs prédécesseurs. Une culture professionnelle efficace reflète la capacité de groupes professionnels à faire la différence entre questions de performance de sécurité et questions contractuelles ou industrielles. Une saine culture professionnelle peut être caractérisée comme la capacité qu'ont tous les groupes professionnels au sein de l'organisation de s'occuper en collaboration des questions de performance de sécurité.

2.6.11 La *culture nationale* différencie les caractéristiques des différentes nations, notamment le rôle de l'individu au sein de la société, la manière dont l'autorité est distribuée et les priorités nationales en ce qui concerne les ressources, les responsabilités, la moralité, les objectifs et les différents régimes juridiques. Dans la perspective de la gestion de la sécurité, la culture nationale joue un grand rôle pour déterminer la nature et la portée des politiques d'application des règlements, y compris les relations entre le personnel de l'autorité réglementaire et le personnel de l'industrie, et la mesure dans laquelle les renseignements sur la sécurité sont protégés.

2.6.12 La culture nationale est un élément intrinsèque des convictions personnelles qui façonne les perspectives des individus sur la sécurité avant qu'ils deviennent membres d'une organisation. La culture organisationnelle peut donc être influencée de façon significative par les cultures nationales présentes chez les membres du personnel de l'organisation.

2.6.13 En appliquant un programme de gestion de la sécurité, les gestionnaires devraient évaluer et considérer de près les différences dans les cultures nationales de leur personnel. Par exemple, la perception des risques de sécurité peut différer grandement entre différentes cultures nationales. Il peut être nécessaire que les aspects relatifs à la sécurité, notamment les styles de communication et de leadership, ainsi que les interactions entre supérieurs et subordonnés, tiennent compte d'un effectif multiculturel.

2.6.14 La *culture de compte rendu* émerge des convictions et des attitudes personnelles en ce qui concerne les avantages et les inconvénients qui peuvent être associés aux systèmes de compte rendu et l'effet ultime sur l'acceptation ou l'utilisation de ces systèmes. Grandement influencée par les cultures organisationnelle, professionnelle et nationale, elle est l'un des critères pour juger de l'efficacité d'un système de sécurité. Une saine culture de compte rendu vise à distinguer entre écarts intentionnels et non intentionnels et à déterminer la meilleure façon de procéder, pour l'organisation dans son ensemble, aussi bien que pour les individus directement concernés.

2.6.15 Le succès d'un système de compte rendu dépend du flux continu d'information venant du personnel de première ligne. Des politiques qui distinguent les fautes intentionnelles des erreurs commises par inadvertance, en prévoyant une réaction appropriée punitive ou non punitive, sont essentielles pour assurer qu'il soit effectivement rendu compte des carences de sécurité systémiques. Une culture « absolument sans blâme » n'est pas seulement déraisonnable, mais n'est même pas réalisable. Le management recevra des informations intéressantes la sécurité, mais le système sera inefficace s'il entrave des actions punitives appropriées. Inversement, une culture qui ne fait pas de distinction entre erreurs/fautes non intentionnelles et actions fautives délibérées entravera le processus de compte rendu. Si le personnel évite de rendre compte par crainte d'être puni, le management ne recevra pas certains renseignements qui sont importants pour la sécurité.

2.6.16 Dans l'ensemble, le personnel doit être convaincu qu'il sera appuyé dans toutes décisions prises dans l'intérêt de la sécurité, mais il doit aussi comprendre que des violations intentionnelles de la politique de sécurité ne seront pas tolérées. C'est pourquoi un système de compte rendu volontaire devrait être confidentiel et fonctionner en accord avec des politiques non punitives appropriées. Le système devrait aussi apporter au personnel un retour d'information sur les améliorations réalisées en matière de sécurité comme résultat des comptes rendus reçus. Cet objectif exige un accès sûr et aisé aux systèmes de compte rendu de sécurité, une collecte active de données de sécurité et un traitement proactif des données par le management.

2.6.17 Les renseignements sur la sécurité devraient être recueillis uniquement pour l'amélioration de la sécurité de l'aviation, et la protection des informations est essentielle pour assurer que ces informations continuent d'être disponibles. Ceci peut être réalisé au moyen d'un système de compte rendu de sécurité qui soit confidentiel, volontaire et non punitif. Les avantages sont doubles. Souvent, les personnels sont au plus près des dangers pour la sécurité, de sorte que le système de compte rendu leur permet d'identifier activement ces dangers. En même temps, le management est en mesure de recueillir des renseignements pertinents sur les dangers pour la sécurité et aussi d'édifier la confiance chez le personnel.

2.6.18 Une fois les données recueillies et stockées, ces renseignements devront être traités pour étayer les mesures appropriées de mise en œuvre, qui devraient être communiquées en temps utile au personnel de première ligne.

Promotion et évaluation d'une culture de sécurité

2.6.19 L'utilisation de métriques tangibles permet de vraiment mesurer et surveiller l'efficacité d'une culture de sécurité. Dans un contexte où la culture de sécurité est à maturité, il peut être escompté que les organisations seront en mesure d'introduire un mécanisme pour mener une évaluation interne de la culture de sécurité de l'organisation (OSC).

Une telle évaluation pourra être encore renforcée en utilisant l'évaluation, plus techniquement impliquée et spécifique à un secteur, dite profil de risque de l'organisation (ORP). Parallèlement, les organismes de l'industrie ou les régulateurs peuvent envisager de développer des dispositifs promotionnels (p. ex. un prix de la culture de sécurité) destinés à encourager des fournisseurs de produits et de services à participer à une évaluation OSC/ORP volontaire de leurs organisations. Les paramètres à évaluer dans une OSC/ORP devraient inclure des facteurs organisationnels et des résultats allant au-delà des exigences réglementaires classiques, mais néanmoins pertinents pour la culture de sécurité d'une organisation, et ayant donc un impact sur ses performances de sécurité. Tel est le rôle principal d'une évaluation OSC/ORP. Elle sert de complément à la supervision réglementaire traditionnelle en s'attendant à des facteurs organisationnels (conditions latentes) qui sont autrement en dehors du domaine de la réglementation. Une liste de vérification pour l'évaluation OSC aurait tendance à être plus générique dans son contenu, alors qu'une liste de vérification ORP serait plus adaptée à la nature des opérations de l'organisation. L'Appendice 1 présente une illustration d'une liste de vérification possible pour une évaluation OSC/ORP spécifique à un secteur.

2.7 LE DILEMME DE LA GESTION

2.7.1 Les processus de gestion de la sécurité identifient des dangers qui comportent le potentiel de compromettre la sécurité. Ils apportent aussi des mécanismes efficaces et objectifs pour évaluer le risque que présentent les dangers et pour mettre en œuvre des moyens d'éliminer ces dangers ou d'atténuer les risques qui leur sont associés. Le résultat de ces processus sera de faciliter la réalisation d'un niveau de sécurité acceptable tout en équilibrant l'affectation des ressources entre production et protection. Dans une perspective d'affectation de ressources, le concept d'espace de sécurité est particulièrement utile pour décrire comment cet équilibre est réalisé.

Espace de sécurité

2.7.2 Dans tout organisme fournisseur de services, risques de production et risques de sécurité sont liés. Lorsque la production s'accroît, les risques de sécurité peuvent aussi s'accroître si les ressources ou les améliorations des processus nécessaires ne sont pas disponibles. Une organisation doit définir ses objectifs de production et ses objectifs de sécurité en recherchant un équilibre entre la production et les risques de sécurité acceptables. Il faut aussi que l'organisation, lorsqu'elle définit ses objectifs de production, définisse des défenses pour garder sous contrôle les risques de sécurité. Pour un fournisseur de produits ou de services, les défenses fondamentales de la sécurité sont la technologie, la formation et les processus et procédures internes. Pour l'État, les défenses fondamentales sont semblables, à savoir formation du personnel, usage approprié de la technologie, supervision effective et processus et procédures internes qui sous-tendent la supervision. L'espace de sécurité est la zone au sein de laquelle une organisation recherche un équilibre entre la production souhaitée et le maintien de la protection de la sécurité nécessaire au moyen de contrôles des risques de sécurité. Un constructeur ou un fournisseur de services de navigation aérienne pourrait, par exemple, souhaiter stimuler la croissance prévue par des investissements dans les nouvelles technologies. Ces technologies peuvent apporter simultanément les améliorations de l'efficacité qui sont nécessaires et des améliorations de la fiabilité et de la performance de sécurité. Une telle prise de décision devrait comporter à la fois une évaluation de la valeur ajoutée aux objectifs de l'organisation en matière de produits ou de services et une évaluation des risques de sécurité que cela implique. Affecter des ressources excessives à la protection ou au contrôle des risques pourrait avoir pour résultat que les produits ou les services deviennent non rentables, ce qui compromettrait la viabilité de l'organisation.

2.7.3 Par ailleurs, l'attribution de ressources excessives à la production, aux dépens de la protection, pourrait avoir un impact sur les performances de sécurité du produit ou des services et aboutir en définitive à un accident. Il est donc indispensable de définir une limite de l'espace de sécurité qui avertisse assez tôt qu'une situation d'affectation déséquilibrée de ressources est en train de se développer ou existe déjà. Les limites de l'espace de sécurité devraient donc être définies par le management de l'organisation et être constamment réexaminées pour s'assurer qu'elles reflètent exactement la situation existante. La Figure 2-6 présente une illustration des limites de l'espace de sécurité d'une organisation.

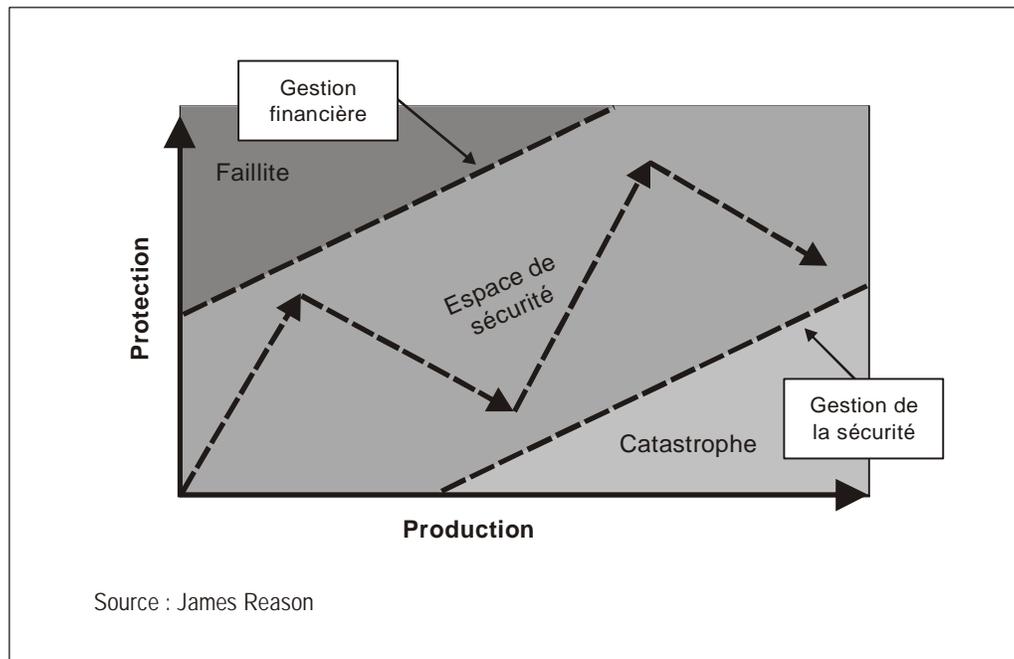


Figure 2-6. L'espace de sécurité

2.7.4 La nécessité d'équilibrer production et protection est devenue une exigence qui est aisément comprise et acceptée dans la perspective d'un fournisseur de produits ou de services. Cet équilibre est également applicable à la gestion par l'État de son PNS, vu le besoin d'équilibrer les ressources nécessaires pour les fonctions étatiques de protection, qui incluent la certification et la surveillance.

2.8 GESTION DU CHANGEMENT

2.8.1 Les organismes d'aviation, y compris les autorités de réglementation, connaissent le changement du fait de l'expansion ou de la contraction ainsi que des modifications apportées à des systèmes, équipements, politiques, programmes, services et règlements existants. Des dangers peuvent être introduits par inadvertance dans le système d'aviation lorsqu'un changement se produit. Les processus de référence existants pour l'atténuation des risques de sécurité peuvent aussi être influencés. Les pratiques de gestion de la sécurité exigent que les dangers résultant du changement soient systématiquement identifiés, et que des stratégies de gestion des risques de sécurité en résultant soient élaborées, mises en œuvre et évaluées par la suite. Une saine gestion des risques de sécurité afférents au changement est une exigence critique des PNS et des SGS.

2.8.2 La gestion des risques de sécurité résultant du changement devrait tenir compte des trois considérations suivantes :

- a) *Caractère critique des systèmes et des activités.* Le caractère plus ou moins critique est en rapport avec les conséquences possibles du risque de sécurité, qu'il s'agisse de les prendre en considération au cours du processus de conception du système ou lors d'une situation liée à un changement systémique. Il y a lieu d'examiner les modifications apportées à des équipements ou à des activités associées à des risques de sécurité relativement élevés pour s'assurer que les mesures correctives nécessaires pourront être prises afin de contrôler les risques de sécurité qui pourraient émerger.

- b) *Stabilité des systèmes et contextes opérationnels.* Les changements peuvent être planifiés et être sous le contrôle direct de l'organisation. Des changements planifiés peuvent être associés à une croissance ou à une contraction de l'organisation, aussi bien qu'à l'introduction de nouveaux équipements, produits ou services. Les changements non planifiés, y compris les changements de nature opérationnelle, politique ou économique, peuvent aussi créer des risques qui exigent une atténuation par l'organisme. Dans des cas où se produisent des changements systémiques ou environnementaux fréquents, les gestionnaires devront actualiser les évaluations des risques clés et les informations connexes plus fréquemment que dans des situations plus stables.
- c) *Performance passée.* La performance passée de systèmes critiques peut être un indicateur fiable de la performance future. Des analyses de tendances dans le processus d'assurance de la sécurité devraient être employées pour suivre au fil du temps les mesures des performances de sécurité et factoriser ces informations pour la planification d'activités futures en situations de changement. De plus, lorsque des carences ont été constatées et corrigées à la suite d'audits, d'évaluations, d'analyses de données, d'investigations ou de comptes rendus passés, il est indispensable que ces informations soient prises en considération pour s'assurer de l'efficacité des mesures correctives.

2.9 INTÉGRATION DES SYSTÈMES DE GESTION

2.9.1 Il existe de grandes variations entre les organisations d'aviation dans leur taille globale et leur complexité. Chacune d'elles a un système de gestion en plusieurs couches, composé de sous-systèmes multiples auxquels un certain type de système de gouvernance donne une orientation. L'organisation devrait intégrer des systèmes de gestion organisationnelle conçus pour la réalisation d'objectifs organisationnels spécifiques, à savoir fournir aux clients des produits et des services. Un système holistique de gestion organisationnelle est souvent appelé système de gestion intégré ou, simplement, « système de management » organisationnel.

2.9.2 Les systèmes de gestion typiques au sein d'une organisation d'aviation peuvent inclure :

- a) un système de gestion de la qualité (SGQ) ;
- b) un système de gestion de la sécurité (SGS) ;
- c) un système de gestion de la sûreté (SGSûr) ;
- d) un système de gestion de l'environnement (SGE) ;
- e) un système de gestion des risques de santé et de sécurité au travail (SGSST) ;
- f) un système de gestion financière (SGF) ;
- g) un système de gestion des documents (SGD).

2.9.3 Chaque système de gestion est surveillé par un « responsable » (*accountable leader*). Des organismes complexes de production de produits ou de services peuvent avoir plus de 30 systèmes de gestion, qui doivent être intégrés dans l'entreprise. Ce sont, par exemple :

- a) un système de gestion des fournisseurs ;
- b) un système de gestion du marketing ;
- c) un système de gestion du personnel ;

- d) un système de gestion des installations ;
- e) un système de gestion de l'équipement au sol ;
- f) un système de gestion de la production ;
- g) un système de gestion de la formation ;
- h) un système de gestion des opérations aériennes ;
- i) un système de gestion des opérations de fret ;
- j) un système de gestion de la maintenance des aéronefs ;
- k) un système de gestion du centre de coordination des opérations ;
- l) un système de gestion des risques de fatigue (SGRF).

2.9.4 Il existe une tendance grandissante dans l'aviation civile à intégrer tous ces systèmes de gestion comme éléments fonctionnels du système global de management d'entreprise. Une telle intégration présente plusieurs avantages clairs :

- a) réduction des doublons, et donc des coûts ;
- b) réduction des risques organisationnels globaux et accroissement de la rentabilité ;
- c) réalisation d'un équilibre entre des objectifs qui pourraient être en conflit ;
- d) élimination de responsabilités et de relations qui pourraient être conflictuelles.

2.9.5 Chaque organisation intégrera ces systèmes sur la base de ses propres exigences de production. Les processus de gestion des risques sont des éléments essentiels des systèmes SGS, SGQ, SGE, SGF, SGSST et SGSûr. Si le SGS fonctionnait isolément de ces autres systèmes de gestion, il pourrait y avoir une tendance à se focaliser seulement sur les risques de sécurité, sans comprendre la nature des menaces pour l'organisation aux niveaux de la qualité, de la sûreté ou de l'environnement.

2.9.6 Actuellement, les SARP harmonisées de l'OACI relatives à la gestion de la sécurité et le présent manuel ne portent pas sur l'intégration du système, mais de nombreuses autorités de l'aviation civile et de nombreux fournisseurs de produits ou de services se sont rendu compte des avantages de l'intégration et de l'alignement de systèmes de gestion multiples. Pour plus de précisions sur l'intégration des SGS et des SGQ, voir le Chapitre 5.

2.10 COMPTES RENDUS ET INVESTIGATIONS SUR LA SÉCURITÉ

Efficacité des comptes rendus sur la sécurité

2.10.1 Rendre compte avec précision et en temps utile des informations pertinentes relatives aux dangers, aux incidents ou aux accidents est une activité fondamentale de gestion de la sécurité. Les données utilisées à l'appui des analyses de sécurité sont communiquées par des sources multiples. Une des meilleures sources de données est la communication directe par le personnel de première ligne, car celui-ci observe les dangers dans le cadre de ses activités quotidiennes. Un lieu de travail où le personnel a été formé et est constamment encouragé à rendre compte de ses erreurs et de ses expériences est une condition requise pour des comptes rendus de sécurité efficaces.

2.10.2 Cinq caractéristiques fondamentales sont universellement associées à des systèmes efficaces de compte rendu de sécurité (voir la Figure 2-7). Des comptes rendus efficaces des dangers sont un élément clé de la gestion de la sécurité. Une fois communiquées, les données sur les dangers pourront être analysées avec d'autres sources de données pour appuyer les processus GRS et AS.

2.10.3 Une autre source de données utilisée à l'appui des processus GRS et AS est le compte rendu d'occurrence. Cela peut aller des événements ayant les plus graves conséquences (accidents, incidents graves) à des événements ayant de moindres conséquences, comme les incidents opérationnels et les défaillances ou défauts de systèmes ou d'équipements. Des exigences réglementaires de compte rendu obligatoire des événements à conséquences graves (accidents, incidents graves) sont courantes, mais un environnement de gestion de la sécurité à maturité prévoit également des comptes rendus d'événements ayant de moindres conséquences. Cela permettra que les mécanismes de surveillance nécessaires portent sur tous les résultats à conséquences graves possibles. La tendance (taux d'occurrence) d'événements ayant de moindres conséquences est inévitablement un précurseur de résultats à conséquences plus graves à venir.

2.10.4 De plus amples éléments d'orientation sur les systèmes de compte rendu des États, volontaires ou obligatoires, figurent dans les Appendices 2 et 3, respectivement, au Chapitre 4. L'Appendice 5 au Chapitre 5 contient des éléments d'orientation sur les systèmes de compte rendu volontaire d'un SGS.

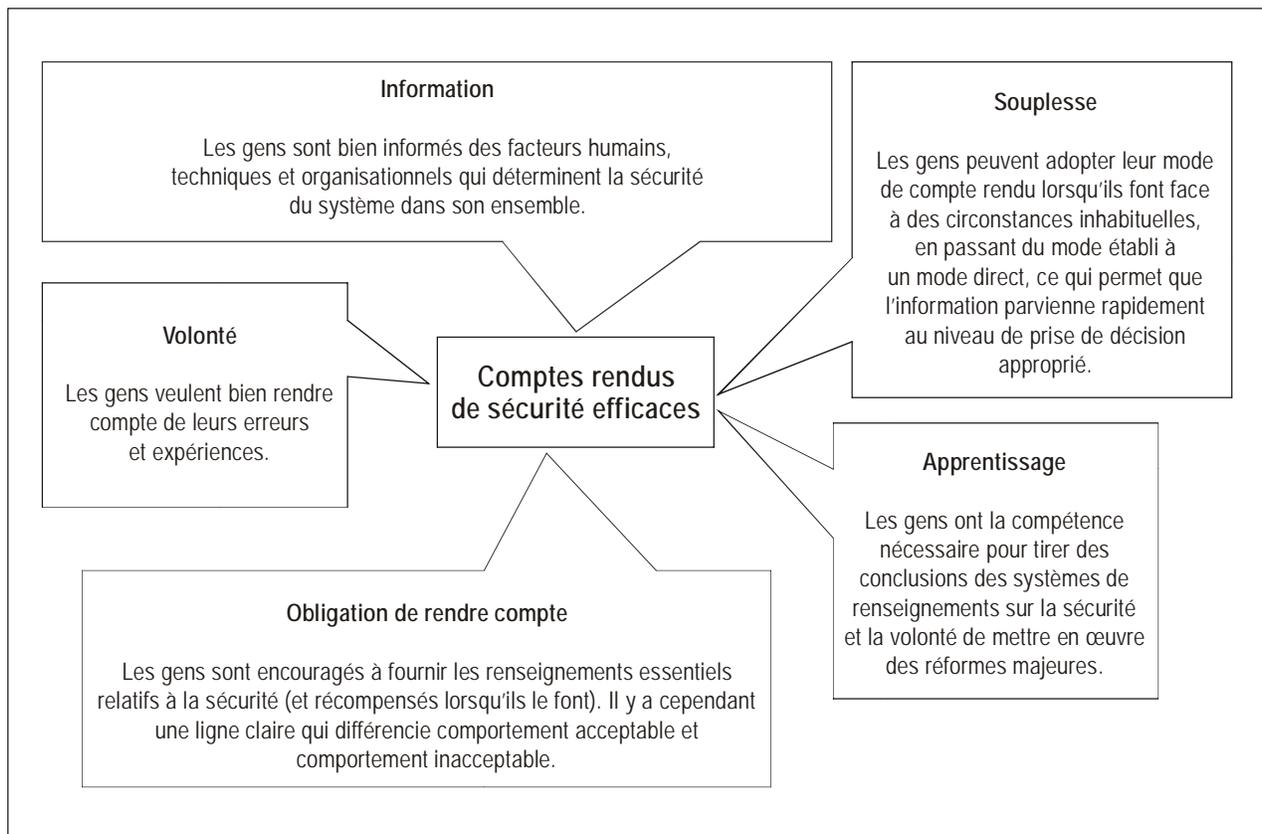


Figure 2-7. Des comptes rendus de sécurité efficaces — cinq caractéristiques de base

Investigations sur les accidents et incidents

2.10.5 Lorsque se produit un accident ou un incident grave, le processus d'investigations sur les accidents est mis en marche pour découvrir toute défaillance possible dans le système d'aviation, avec ses raisons, et générer les contre-mesures nécessaires pour éviter qu'elle se reproduise. Ainsi, dans un contexte de gestion de la sécurité, le processus d'enquête sur les accidents a un rôle distinct, étant un processus essentiel qui se déploie lorsque les défenses de sécurité, barrières, contrôles et contrepoids que comporte le système ont échoué.

2.10.6 Étant une composante réactive importante des éléments constitutifs des cadres SGS et PNS, les investigations sur les accidents contribuent à l'amélioration continue du système d'aviation en mettant en évidence les causes profondes des accidents/incidents et les enseignements tirés de l'analyse des événements. Ceci peut appuyer des décisions relatives à l'élaboration d'actions correctives et l'attribution de ressources correspondantes, et peut aider à identifier les améliorations à apporter au système d'aviation, y compris au SGS, au PNS et au processus national d'investigations sur les accidents. Il est courant que les investigations obligatoires à l'échelon des États soient limitées aux accidents et aux incidents graves, mais un environnement de gestion de la sécurité à maturité pourra prévoir aussi des investigations sur des événements à moindres conséquences.

2.10.7 En plus d'établir des constatations et de déterminer les causes profondes des accidents/incidents, la plupart des activités d'investigations découvrent aussi des dangers/menaces. Un processus d'investigations efficace et complet identifie et distingue une conséquence ultime, un événement dangereux et les dangers/menaces contribuant à l'accident/incident. Ceci peut inclure tous facteurs systémiques, latents ou organisationnels au sein du cadre du système d'aviation dans son ensemble. Dans l'environnement proactif actuel de gestion de la sécurité, l'intégration entre le processus d'investigations sur les accidents/incidents d'une organisation et son processus de compte rendu/d'identification des dangers est importante et nécessaire. Les formulaires de compte rendu d'investigations devraient comporter une disposition indiquant clairement l'obligation de documenter les dangers/menaces découverts au cours du processus d'investigations qui exigeraient des mesures de suivi séparées au niveau des processus de l'organisation pour l'identification des dangers et pour l'atténuation des risques. Il est courant que certains comptes rendus d'investigations limitent leurs « conclusions » et les « mesures prises/recommandées » aux causes immédiates ou directes seulement. Ainsi, des dangers/menaces secondaires ou indirects auraient tendance à être négligés, à moins que cette lacune puisse être surmontée en reliant les processus d'investigations sur les accidents/incidents et les processus d'identification des dangers.

2.11 COLLECTE ET ANALYSE DES DONNÉES SUR LA SÉCURITÉ

Collecte et qualité des données sur la sécurité

2.11.1 La prise de décision basée sur les données est l'un des aspects les plus importants de tout système de gestion. Le type de données sur la sécurité à recueillir peut inclure les comptes rendus sur les accidents et incidents, événements, cas de non-conformité ou d'écart et comptes rendus de dangers. La qualité des données qui sont utilisées pour permettre une prise de décision efficace doit être considérée tout au cours du développement et de la mise en œuvre des PNS et SGS. Malheureusement, de nombreuses bases de données n'ont pas la qualité de données nécessaire pour servir de base fiable pour évaluer les priorités en matière de sécurité et l'efficacité des mesures d'atténuation des risques. S'il n'était pas tenu compte des limites des données utilisées pour appuyer les fonctions de gestion des risques de sécurité et d'assurance de la sécurité, il en résulterait des résultats d'analyse défectueux qui pourraient mener à des décisions erronées et discréditer le processus de gestion de la sécurité.

2.11.2 Vu l'importance de la qualité des données, les organisations devront évaluer sur la base des critères suivants les données utilisées à l'appui des processus de gestion des risques de sécurité et d'assurance de la sécurité :

- a) *Validité*. Les données recueillies sont acceptables selon les critères établis pour l'usage auquel elles sont destinées.
- b) *Exhaustivité*. Aucune donnée pertinente n'est manquante.
- c) *Cohérence*. Le degré de cohérence de la mesure d'un paramètre donné peut être reproduit et évite l'erreur.
- d) *Accessibilité*. Les données sont aisément disponibles pour analyse.
- e) *Rapidité*. Les données se rapportent à la période d'intérêt et sont promptement disponibles.
- f) *Sûreté*. Les données sont protégées contre l'altération par inadvertance ou malveillance.
- g) *Exactitude*. Les données sont exemptes d'erreurs.

En considérant ces sept critères de qualité des données, les analyses de données sur la sécurité produiront les renseignements de la plus grande exactitude possible pour être utilisés à l'appui de la prise de décision stratégique.

Base de données de sécurité

2.11.3 Dans le contexte de la collecte et de l'analyse des données de sécurité, le terme « base de données de sécurité » peut inclure les types suivants de données ou de renseignements qui pourront être utilisés à l'appui de l'analyse des données sur la sécurité :

- a) données d'investigations sur accidents ;
- b) données d'investigations obligatoires sur des incidents ;
- c) données de comptes rendus volontaires ;
- d) données de comptes rendus de maintien de la navigabilité ;
- e) données de surveillance de la performance opérationnelle ;
- f) données d'évaluation des risques ;
- g) données de constatations/comptes rendus d'audits ;
- h) données d'études/examens de la sécurité ;
- i) données sur la sécurité provenant d'autres États, d'organisations régionales de supervision de la sécurité (RSOO) ou d'organisations régionales d'enquête sur les accidents et incidents (RAIO), etc.

2.11.4 Une base de données de sécurité peut être, selon le contexte, une base de données se rapportant au PNS de l'État ou une base de données relatives au SGS interne d'un prestataire de services. Des comptes rendus volontaires peuvent provenir du personnel opérationnel (prestataires de services, pilotes, etc.), mais aussi de passagers ou du public en général.

2.11.5 Beaucoup des données des bases de données de sécurité sont présentées sous forme de comptes rendus relatifs à des événements complexes, tels que des accidents et incidents. Les comptes rendus figurant dans ces

types de bases de données répondent généralement à une série de questions. Qui est impliqué dans l'événement ? Que s'est-il passé, qui a causé la rédaction d'un compte rendu ? Quand l'événement s'est-il produit ? Pourquoi s'est-il produit ? Où a-t-il eu lieu ? D'autres types de bases de données sont liées à des questions relativement étroites, telles que l'information de vol, les renseignements météorologiques et les volumes de trafic. Ces comptes rendus portent sur des faits simples.

2.11.6 Les bases de données de sécurité sont généralement hébergées dans diverses parties d'une organisation. De nombreuses organisations donnent accès aux bases de données à travers une interface qui permet aux analystes de la sécurité de spécifier efficacement et d'extraire les comptes rendus qui les intéressent. Les comptes rendus peuvent être examinés individuellement ou collectivement par agrégation. Des outils d'analyse permettent aux analystes de la sécurité d'examiner sous des formes multiples les données extraites. Il peut s'agir, par exemple, de feuilles de calcul, de cartes et de divers types de graphiques.

2.11.7 Pour assurer qu'une base de données soit comprise et utilisée comme il convient, il faut que les renseignements relatifs à cette base de données (métadonnées) soient bien documentés et mis à la disposition des usagers. Les types de métadonnées comprennent les définitions de champs, les modifications apportées au fil du temps à la base de données, les règles d'utilisation, le formulaire de collecte de données et des références à des valeurs valables.

2.11.8 Un grand nombre de bases de données de sécurité ont été développées de façon indépendante par de nombreuses organisations différentes, ayant des domaines de responsabilité et des besoins d'analyse très différents. Pour fournir aux analystes de la sécurité de l'aviation une vision élargie des questions de sécurité, il est nécessaire d'édifier des dispositifs d'intégration des renseignements sur la sécurité qui pourront extraire des informations de sources multiples, appliquer des normes communes relatives aux données, regrouper les métadonnées et charger les informations sur une plate-forme commune hébergée dans une architecture centralisée de stockage des données.

2.11.9 Une fois traitées, les données de sécurité sont rendues accessibles aux analystes de la sécurité au moyen d'une interface commune et d'un ensemble commun d'outils d'analyse. Si un analyste a besoin de données de bases de données multiples, l'application de normes communes relatives aux données permet aux techniciens de base de données d'extraire les données nécessaires et de construire une base de données entièrement nouvelle. La Figure 2-8 donne une vision schématique d'un système national de données de sécurité, indiquant les éléments d'entrée, les processus et les éléments de sortie relatifs à la collecte, à l'analyse et à l'échange de données sur la sécurité.

Analyse des données de sécurité

2.11.10 Après avoir recueilli de diverses sources les données de sécurité, les organisations devraient effectuer l'analyse nécessaire pour identifier les dangers et maîtriser leurs conséquences possibles. Parmi d'autres finalités, l'analyse pourra être utilisée pour :

- a) aider à décider quels faits additionnels sont nécessaires ;
- b) déterminer les facteurs latents sous-jacents aux carences en matière de sécurité ;
- c) aider à parvenir à des conclusions valides ;
- d) surveiller et mesurer les tendances ou les performances en matière de sécurité.

2.11.11 L'analyse de la sécurité est souvent itérative, exigeant des cycles multiples. Elle peut être quantitative ou qualitative. L'absence de données de référence quantitatives peut obliger à s'en remettre à des méthodes d'analyse plus qualitatives.

2.11.12 Le jugement humain peut être sujet à un certain niveau de biais sur la base d'expériences passées, qui peuvent influencer l'interprétation de résultats d'analyse ou la mise à l'épreuve d'hypothèses. Une des formes les plus fréquentes d'erreur de jugement est le « biais de confirmation ». C'est la tendance à rechercher et retenir les informations qui confirment ce que l'on croit déjà être vrai.

Éléments d'entrée (Collecte)	<ul style="list-style-type: none"> • comptes rendus d'accidents et d'incidents ; • systèmes volontaires de compte rendu d'incident ; • systèmes obligatoires de compte rendu d'incident ; • systèmes de collecte de données opérationnelles (provenant directement de prestataires de services) ; • systèmes de collecte de données de supervision de la sécurité.
Processus (Analyse)	<ul style="list-style-type: none"> • outils de collecte de données et de gestion des données pour saisir et stocker les données provenant de : <ul style="list-style-type: none"> — systèmes de compte rendu d'accidents et d'incidents ; — systèmes opérationnels de collecte de données ; — systèmes de collecte de données de supervision de la sécurité ; — recommandations issues d'investigations sur des accidents et des incidents graves ; • méthodes d'analyse pour évaluer les risques connus et émergents à partir de toutes les sources de données disponibles ; • indicateurs de sécurité, niveaux visés et niveaux d'alerte (niveau individuel ou agrégé) pour mesurer la performance de sécurité et détecter les tendances indésirables ; • élaboration de processus de surveillance de la sécurité basés sur les risques, y compris la priorisation des inspections et des audits.
Éléments de sortie (Échange)	<ul style="list-style-type: none"> • recommandations de sécurité publiées par les autorités nationales compétentes sur la base de tous les éléments d'entrée du système de données de sécurité ; • rapports sur les indicateurs, objectifs et alertes de sécurité (au niveau des fournisseurs de services et au niveau de l'État) générés par l'analyse des entrées de données, notamment : <ul style="list-style-type: none"> — analyses comparatives « de référence » (<i>benchmark</i>) ; — analyses de tendances historiques ; — corrélations entre indicateurs proactifs et dénouements en matière de sécurité (accidents et incidents graves) ; • revues des règlements et processus de supervision de l'État, y compris la priorisation des activités de supervision selon les domaines de plus grand risque ; • mesures administratives nécessaires à des fins de sécurité ; • échange de renseignements relatifs aux questions de sécurité entre autorités nationales de réglementation et autorités d'enquête sur les accidents ; • échange de renseignements sur les questions de sécurité entre prestataires de services, autorités de réglementation et organismes d'enquête sur les accidents et incidents, aux échelons national, régional et international.

Figure 2-8. Vision schématique d'un système national de données de sécurité

Méthodes et outils d'analyse

2.11.13 Les méthodes suivantes peuvent être utilisées pour l'analyse de la sécurité :

- a) *Analyse statistique.* Cette méthode peut être utilisée pour évaluer l'importance de tendances perçues en matière de sécurité, souvent décrites dans des présentations graphiques de résultats d'analyse. L'analyse statistique peut fournir de puissantes informations concernant la signification de certaines tendances, mais il faut considérer avec soin la qualité des données et les méthodes d'analyse pour éviter de parvenir à des conclusions erronées.
- b) *Analyse de tendances.* En surveillant les tendances dans les données de sécurité, on pourra faire des prédictions au sujet d'événements futurs. Les tendances peuvent être indicatives de dangers émergents.
- c) *Comparaisons normatives.* Il est possible que les données disponibles ne soient pas suffisantes pour fournir une base factuelle, à laquelle comparer les circonstances d'événements possibles. Dans de tels cas, il pourra être nécessaire d'échantillonner des expériences du monde réel dans des conditions d'exploitation similaires.
- d) *Simulation et tests.* Dans certains cas, des dangers peuvent devenir évidents au travers de simulations aussi bien que de tests en laboratoire pour valider les incidences, en matière de sécurité, de types nouveaux d'opérations, d'équipement ou de procédures.
- e) *Groupe d'experts.* Les avis de pairs et de spécialistes peuvent être utiles pour évaluer la nature diverse des dangers en rapport avec une certaine situation dangereuse. Une équipe multidisciplinaire formée pour évaluer les indices d'une situation dangereuse pourra aider à identifier la meilleure façon de procéder pour les mesures correctives.
- f) *Analyse coûts-avantages.* L'acceptation de mesures recommandées pour la maîtrise des risques de sécurité peut dépendre d'une analyse coûts-avantages crédible. Le coût de la mise en œuvre des mesures proposées est soupesé par rapport aux avantages attendus au fil du temps. Une analyse coûts-avantages pourra donner à penser que l'acceptation des conséquences du risque de sécurité est tolérable si l'on considère le temps, les efforts et les dépenses qu'exigerait la mise en œuvre des mesures correctives.

Gestion des renseignements sur la sécurité

2.11.14 Une gestion efficace de la sécurité est « tirée par les données ». Une bonne gestion des bases de données de l'organisme est fondamentale pour assurer une analyse de sécurité efficace et fiable des sources de données regroupées.

2.11.15 L'établissement et la tenue d'une base de données de sécurité fournissent un outil essentiel pour le personnel qui surveille les questions de sécurité du système. On peut trouver dans le commerce une large gamme de bases de données électroniques peu coûteuses, capables de prendre en charge les besoins de l'organisation en matière de gestion des données.

2.11.16 Selon la taille et la complexité de l'organisation, les besoins du système peuvent inclure un éventail de fonctionnalités pour gérer efficacement les données de sécurité. D'une manière générale, le système devrait :

- a) inclure une interface conviviale pour la saisie de données et les demandes ;

- b) avoir la capacité de transformer de grandes quantités de données sur la sécurité en renseignements utiles pour appuyer la prise de décisions ;
- c) réduire la charge de travail pour les cadres et le personnel de sécurité ;
- d) fonctionner à relativement faible coût.

2.11.17 Pour tirer parti des avantages que peuvent apporter les bases de données de sécurité, une compréhension élémentaire de leur fonctionnement est nécessaire. Toutes informations regroupées de manière organisée pourraient être considérées comme constituant une base de données, mais l'analyse de dossiers papier conservés dans un système de classement simple ne suffirait que pour de petites opérations. La conservation, l'enregistrement, le rappel et l'extraction en utilisant des systèmes papier sont des tâches lourdes. Les données de sécurité devraient de préférence être stockées dans une base de données électronique qui facilite l'interrogation des dossiers et la production de résultats d'analyse sous diverses formes.

2.11.18 Les propriétés et les attributs fonctionnels de différents systèmes de gestion de bases de données varient, et chacun d'eux devrait être considéré avant de décider du système le plus approprié. Les éléments de base devraient permettre à l'utilisateur d'accomplir des tâches telles que :

- a) classer des événements de sécurité dans différentes catégories ;
- b) relier des événements à des documents apparentés (p. ex. rapports et photographies) ;
- c) surveiller des tendances ;
- d) compiler des analyses, cartes et rapports ;
- e) vérifier des antécédents ;
- f) partager des données de sécurité avec d'autres organisations ;
- g) surveiller des investigations sur des événements ;
- h) surveiller la mise en œuvre d'actions correctives.

Protection des données de sécurité

2.11.19 Vu la possibilité d'utilisation abusive de données de sécurité compilées strictement dans le but de promouvoir la sécurité de l'aviation, la gestion de la base de données devra comprendre la protection de ces données. Les gestionnaires de base de données doivent réaliser un équilibre entre la nécessité de protéger les données et celle de les rendre accessibles à ceux qui peuvent promouvoir la sécurité de l'aviation. Les considérations de protection sont notamment les suivantes :

- a) caractère adéquat des règlements relatifs à « l'accès à l'information » par rapport aux exigences de gestion de la sécurité ;
- b) politiques et procédures opérationnelles relatives à la protection des données de sécurité limitant l'accès à ceux qui « ont besoin de savoir » ;
- c) dépersonnalisation, en éliminant toutes précisions qui pourraient amener un tiers à inférer l'identité de personnes (p. ex. numéros de vol, dates/heures, lieux et types d'avion) ;

- d) sécurisation des systèmes d'information, du stockage des données et des réseaux de communication ;
- e) interdiction d'utilisation non autorisée de données.

L'Appendice 5 au Chapitre 4 contient de plus amples renseignements concernant la protection des données de sécurité.

2.12 INDICATEURS DE SÉCURITÉ ET SURVEILLANCE DES PERFORMANCES

2.12.1 Les extraits du système de collecte et d'analyse des données sont normalement présentés sous forme de graphes ou de graphiques. Normalement utilisés dans les systèmes classiques de gestion de la qualité/fiabilité, ceux-ci montrent généralement un « instantané » de l'analyse de données résultant d'une interrogation unique.

2.12.2 La Figure 2-9 est un diagramme d'analyse de données de base (capture d'écran) ; montrant le nombre absolu d'incidents ayant fait l'objet d'un compte rendu obligatoire d'événement (MOR) par type de flotte pour l'année 2009. Un tel diagramme de base ne montre pas le nombre d'aéronefs dans chacun des types de flotte. Ce type de diagramme ne présente donc qu'un intérêt limité. Il ne serait pas adéquat comme indicateur continu de performance de sécurité.

2.12.3 L'analyse utilisée pour surveiller la sécurité en continu devrait prendre la forme d'une extraction périodique de données pour générer un diagramme ou un graphique de tendance, actualisé mensuellement ou trimestriellement, comme le montre la Figure 2-10. Celle-ci présente des renseignements sur le taux mensuel d'incidents devant faire l'objet d'un compte rendu, en prenant en considération le nombre d'heures de vol (FH) cumulées pour la flotte de l'exploitant. Le téléchargement périodique (mensuel) de données sur le taux d'incidents permettra ensuite que le graphe serve d'indicateur continu de surveillance de tendance. Une fois qu'un tel graphe est en place, la prochaine étape sera de le transformer en indicateur de mesure de performances de sécurité, en fixant à l'intérieur de ce graphe un niveau cible et un niveau d'alerte. Cette étape devrait de préférence être réalisée lorsque des points de données historiques auront déjà été générés sur le graphe. Ces points de données historiques (performance historique) serviront de base pour établir ou définir des niveaux inacceptables de tendance à l'alerte ainsi que tout niveau d'amélioration visé dont la réalisation serait souhaitée au cours d'une période spécifiée. Le Chapitre 4 (PNS) et le Chapitre 5 (SGS) contiennent plus de précisions sur le développement d'indicateurs de performance de sécurité et sur les réglages d'objectif et d'alerte qui leur sont associés.

2.13 DANGERS

2.13.1 L'identification des dangers est un prérequis pour le processus de gestion des risques de sécurité. Toute différenciation inexacte entre dangers et risques de sécurité pourrait être source de confusion. Une compréhension claire des dangers et de leurs conséquences est indispensable à la mise en œuvre d'une bonne gestion des risques de sécurité.

Comprendre les dangers et leurs conséquences

2.13.2 Un danger est défini de manière générique par les praticiens de la sécurité comme une situation ou un objet ayant le potentiel de causer la mort, des lésions au personnel, des dommages aux équipements ou aux structures, la perte de matériel ou une réduction de la capacité d'accomplir une fonction prescrite. Aux fins de la gestion des risques de sécurité en aviation, le terme danger devrait être focalisé sur les conditions qui pourraient causer ou contribuer à causer un fonctionnement peu sûr de l'aéronef ou d'équipements, de produits ou de services en rapport avec la sécurité de l'aviation. (Les paragraphes 2.13.12 et 2.13.13 donnent des indications sur la distinction entre dangers directement pertinents pour la sécurité de l'aviation et autres dangers généraux/industriels.)

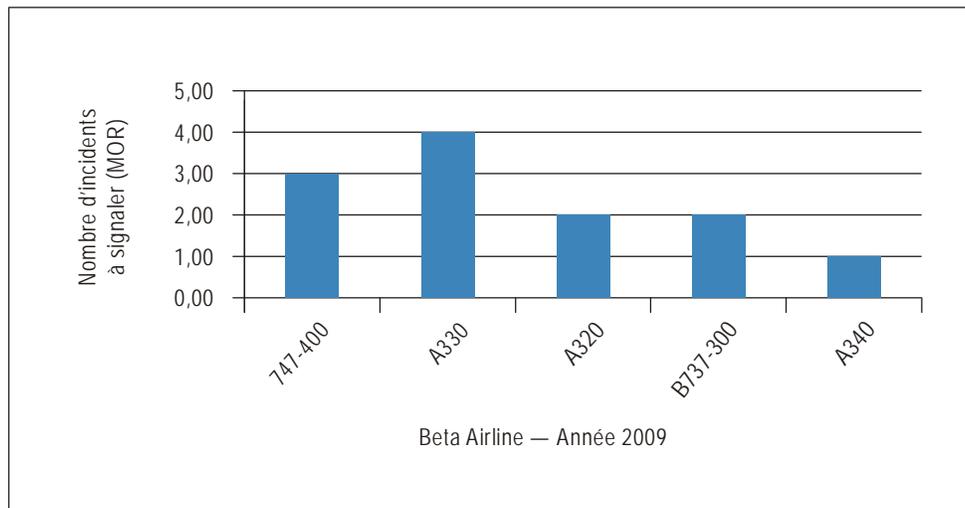


Figure 2-9. Graphe d'analyse des données (capture d'écran) de base

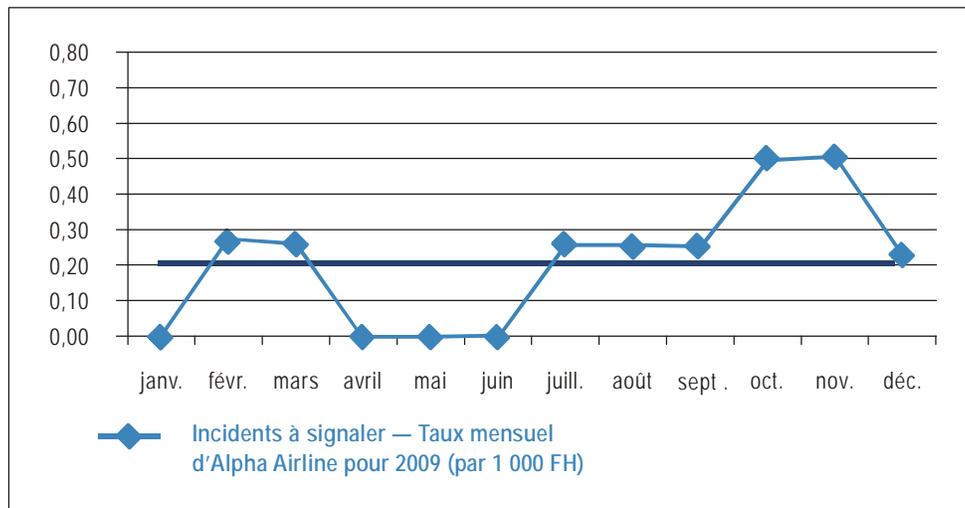


Figure 2-10. Graphe indicateur de sécurité à surveillance continue

2.13.3 Considérons, par exemple, un vent de 15 nœuds qui n'est pas nécessairement une condition dangereuse. En fait, un vent de 15 nœuds soufflant directement vers l'aval de la piste améliore la performance au décollage et à l'atterrissage. Par contre, un vent de 15 nœuds soufflant dans une direction à 90° par rapport à une piste de décollage ou d'atterrissage prévu crée une condition de vent traversier qui peut être dangereuse du fait de son potentiel de contribuer à une occurrence opérationnelle telle qu'une sortie latérale de piste.

2.13.4 Les dangers font inévitablement partie des activités d'aviation. Il est cependant possible de traiter de leurs manifestations et de leurs conséquences possibles par diverses stratégies d'atténuation pour circonscrire la possibilité qu'un danger aboutisse à un fonctionnement peu sûr de l'aéronef ou d'équipements d'aviation.

2.13.5 On a souvent tendance à confondre les dangers avec leurs conséquences ou leurs résultats. Une conséquence est un résultat qui a été déclenché par un danger. Par exemple, une sortie de piste (dépassement) est une conséquence à prévoir en rapport avec le danger que présente une piste contaminée. Si l'on a d'abord clairement défini le danger, on pourra ensuite faire une projection de la conséquence ou du résultat correspondant. Il est à noter que les conséquences peuvent être multicouches, incluant par exemple un événement dangereux intermédiaire avant une conséquence ultime (accident). Voir aussi l'Appendice 2, Tableau 2-A2-3.

2.13.6 Dans l'exemple ci-dessus du vent traversier, un résultat immédiat du danger pourrait être une perte du contrôle latéral, suivie d'une sortie de piste conséquente. La conséquence ultime pourrait être un accident. Le potentiel dommageable d'un danger se concrétise au travers d'une ou plusieurs conséquences. Il est donc important que les évaluations de sécurité comprennent un compte rendu complet de toutes les conséquences probables, décrites avec précision et en termes pratiques. La conséquence la plus extrême, la perte de vie humaine, devrait être différenciée de celles qui comportent le potentiel de moindres conséquences, telles qu'une charge de travail accrue pour l'équipage de conduite, un inconfort pour les passagers ou une réduction des marges de sécurité. La description des conséquences selon leurs résultats plausibles facilitera l'élaboration et la mise en œuvre de stratégies d'atténuation par une priorisation appropriée et une affectation appropriée de ressources, qui sont limitées. Bien identifier les dangers mène à une évaluation appropriée de leurs résultats possibles.

2.13.7 Les dangers devraient être différenciés de l'erreur, composante normale et inévitable de la performance humaine, qui doit être gérée.

Identification et priorisation des dangers

2.13.8 Des dangers existent à tous niveaux dans l'organisation et l'on peut les détecter en utilisant des systèmes de compte rendu, des inspections ou des audits. Des événements fâcheux (*mishaps*) peuvent se produire lorsque des dangers interagissent avec certains facteurs de déclenchement. Les dangers devraient donc être identifiés avant qu'ils ne mènent à des accidents, incidents ou autres événements en rapport avec la sécurité. Un mécanisme important pour une identification proactive des dangers est un système volontaire de compte rendu de danger/d'incident. Le Chapitre 4, Appendice 2, et le Chapitre 5, Appendice 5, donnent plus de renseignements sur les systèmes de compte rendu volontaire. Les informations recueillies grâce à ces systèmes de compte rendu peuvent être complétées par les observations ou constatations enregistrées lors des inspections courantes des sites ou lors des audits de l'organisation.

2.13.9 Les dangers peuvent aussi être identifiés à partir de l'examen ou de l'étude de comptes rendus d'investigations, spécialement les dangers qui sont considérés être des facteurs contributifs indirects et qui pourraient n'avoir pas été abordés convenablement par les actions correctives résultant du processus d'investigations. Ainsi, une procédure systématique consistant à revoir les rapports d'enquête sur les accidents/incidents pour repérer les dangers qui pourraient être passés inaperçus est un bon mécanisme pour renforcer le système d'identification des dangers d'une organisation. Ceci s'applique en particulier si la culture de sécurité d'une organisation n'est pas suffisamment à maturité pour soutenir un système efficace de comptes rendus volontaires de dangers.

2.13.10 Les dangers peuvent être classés en catégories, selon leur source ou leur emplacement. Une priorisation objective des dangers peut exiger un classement par catégories selon la gravité/probabilité de leurs conséquences à prévoir. Cela facilitera la priorisation des stratégies d'atténuation des risques de façon à utiliser de la manière la plus efficace des ressources qui sont limitées. Voir à l'Appendice 3 au présent chapitre un exemple de procédure de priorisation des dangers.

Méthodes d'identification des dangers

2.13.11 Il y a trois méthodes d'identification des dangers :

- a) *Réactive*. Cette méthode repose sur l'analyse de résultats ou d'événements du passé. Les dangers sont identifiés par des investigations sur les événements de sécurité. Les incidents et accidents sont des indicateurs évidents de carences du système et peuvent donc être utilisés pour déterminer les dangers ayant contribué à l'événement ou qui sont latents.
- b) *Proactive*. Cette méthode repose sur l'analyse de situations existantes ou en temps réel, ce qui est la tâche première de la fonction d'assurance de la sécurité, avec ses audits, évaluations, comptes rendus du personnel et processus connexes d'analyse et d'évaluation. Ceci implique de rechercher activement les dangers dans les processus existants.
- c) *Prédictive*. Cette méthode repose sur la collecte de données pour identifier d'éventuels résultats ou événements futurs négatifs et analyser les processus systémiques et l'environnement afin d'identifier de possibles dangers futurs et de lancer des mesures d'atténuation.

Distinguer entre dangers pour l'aviation et dangers pour la sécurité professionnelle, la santé et l'environnement (OSHE)

2.13.12 Comprendre si un danger concerne la sécurité de l'aviation ou s'il s'agit d'un danger OSHE dépend de sa conséquence ou de son risque potentiel ou prévisible. Tout danger qui peut avoir (directement ou indirectement) un impact sur la sécurité d'exploitation d'un aéronef ou d'équipement, de produits ou de services liés à la sécurité de l'aviation devrait être considéré pertinent pour un SGS d'aviation. Un danger ayant des conséquences purement OSHE (c'est-à-dire sans incidences sur la sécurité de l'aviation) devrait être abordé séparément par le système/les procédures OSHE de l'organisation, selon ses exigences OSHE nationales ou organisationnelles. Les dangers et les conséquences OSHE sans impact sur la sécurité de l'aviation ne sont pas pertinents pour un SGS d'aviation.

2.13.13 Les risques de sécurité afférents à des dangers composites ayant simultanément des incidences sur la sécurité de l'aviation et des incidences OSHE pourront être gérés par des processus distincts (parallèles) d'atténuation des risques, pour s'attaquer respectivement aux conséquences pour l'aviation et aux conséquences OSHE. Une autre possibilité est d'utiliser un système intégré d'atténuation des risques pour l'aviation et des risques OSHE pour s'attaquer à de tels dangers composés. Un exemple de danger composé est la foudre qui frappe un aéronef à une porte de transit d'un aéroport. Un inspecteur OSHE pourra considérer qu'il s'agit d'un « danger sur les lieux de travail » (personnel au sol/sécurité des lieux de travail). Pour un inspecteur de la sécurité de l'aviation, il s'agit aussi d'un danger pour l'aviation avec risque de dommages à l'aéronef et risque pour la sécurité des passagers. Les conséquences de tels dangers composés n'étant pas les mêmes au niveau OSHE et au niveau de la sécurité de l'aviation, il convient de prendre dûment en considération le fait qu'il y a lieu de les gérer séparément. La finalité et la focalisation des contrôles préventifs seraient différentes pour les conséquences OSHE et pour les conséquences en matière de sécurité de l'aviation.

2.14 RISQUE DE SÉCURITÉ

2.14.1 La gestion du risque de sécurité est un autre élément clé d'un système de gestion de la sécurité. L'emploi de ce terme entend différencier cette fonction de la gestion de risques financiers, juridiques, économiques, etc. Cette section présente les notions fondamentales en matière de risque de sécurité et porte sur les questions suivantes :

- a) définition du risque de sécurité ;

- b) probabilité du risque de sécurité ;
- c) gravité du risque de sécurité ;
- d) tolérabilité du risque de sécurité ;
- e) gestion du risque de sécurité.

Définition du risque de sécurité

2.14.2 Un risque de sécurité est défini par la probabilité et la gravité projetées de la conséquence ou du résultat d'un danger existant ou d'une situation existante. Le résultat peut être un accident, mais « un événement dangereux/une conséquence dangereuse intermédiaire » peut être identifié comme « résultat le plus crédible ». Assurer l'identification de ces conséquences en couches est généralement associé à des logiciels plus avancés d'atténuation des risques. La feuille de calcul d'atténuation du risque de sécurité présentée à l'Appendice 2 à ce chapitre présente aussi cette disposition.

Probabilité des risques de sécurité

2.14.3 Le processus de maîtrise des risques de sécurité commence par l'évaluation de la probabilité que les conséquences des dangers se concrétisent au cours d'activités d'aviation menées par l'organisation. La probabilité du risque de sécurité est définie comme probabilité ou fréquence d'occurrence d'une conséquence ou d'un résultat en matière de sécurité. Des questions telles que celles qui suivent pourront aider à déterminer cette probabilité :

- a) Existe-t-il un historique d'occurrences similaires à celle qui est considérée ou s'agit-il d'un cas isolé ?
- b) D'autres équipements ou éléments du même type pourraient-ils présenter des défauts semblables ?
- c) Au sein du personnel, quel est le nombre de personnes qui appliquent les procédures considérées ou qui y sont soumises ?
- d) Pendant quel pourcentage du temps l'équipement suspect ou la procédure contestable sont-ils utilisés ?
- e) Dans quelle mesure des incidences au niveau de l'organisation, de la gestion ou de la réglementation pourraient-elles comporter de plus grandes menaces pour la sécurité publique ?

2.14.4 Tous facteurs sous-jacents à ces questions aideront à évaluer la probabilité qu'un danger puisse exister, en prenant en considération tous les scénarios potentiellement valables. La détermination de cette probabilité pourra ensuite aider à déterminer la probabilité de risques de sécurité.

2.14.5 La Figure 2-11 présente un tableau type de probabilité de risque de sécurité, en l'occurrence un tableau en cinq points. Ce tableau comprend cinq catégories, pour indiquer la probabilité que survienne un événement dangereux ou une situation dangereuse, la description de chaque catégorie et l'attribution d'une valeur à chaque catégorie.

2.14.6 Il est à souligner que ceci n'est qu'un exemple et que le niveau de complexité des tableaux et matrices devrait être adapté pour correspondre aux besoins particuliers et aux complexités particulières de différentes organisations. Il est à noter aussi que les organisations peuvent inclure des critères qualitatifs et quantitatifs qui pourront comprendre jusqu'à 15 valeurs.

<i>Probabilité</i>	<i>Signification</i>	<i>Valeur</i>
Fréquent	Susceptible de se produire de nombreuses fois (s'est produit fréquemment)	5
Occasionnel	Susceptible de se produire parfois (ne s'est pas produit fréquemment)	4
Éloigné	Peu susceptible de se produire, mais possible (s'est produit rarement)	3
Improbable	Très peu susceptible de se produire (on n'a pas connaissance que cela se soit produit)	2
Extrêmement improbable	Il est presque inconcevable que l'événement se produise	1

Figure 2-11. Tableau de probabilité d'un risque de sécurité

Gravité d'un risque de sécurité

2.14.7 Une fois achevée l'évaluation de probabilité, la prochaine étape est d'évaluer la gravité du risque de sécurité, en tenant compte des conséquences qui pourraient être liées au danger. La gravité du risque de sécurité est définie comme l'étendue du dommage qui pourrait raisonnablement se produire en conséquence ou comme résultat du danger identifié. L'évaluation de gravité peut être basée sur :

- a) Morts/blessures. Quel pourrait être le nombre de pertes de vies humaines (personnel, passagers, riverains, grand public) ?
- b) Dommages. Quelle serait l'étendue probable des dommages à des aéronefs, à des biens ou à des équipements ?

2.14.8 L'évaluation de la gravité devrait prendre en considération toutes les conséquences possibles en rapport avec une situation peu sûre ou un objet dangereux, en tenant compte de la pire situation prévisible. La Figure 2-12 présente un tableau type de gravité des risques de sécurité. Elle comprend cinq catégories, pour indiquer le niveau de gravité, la description de chaque catégorie, et l'affectation d'une valeur à chaque catégorie. De même que le tableau de probabilité des risques de sécurité, ce tableau n'est qu'un exemple.

Tolérabilité des risques de sécurité

2.14.9 Le processus d'évaluation de la probabilité et de la gravité des risques de sécurité peut être utilisé pour en tirer un indice de risque de sécurité. L'indice créé par la méthode décrite ci-dessus est constitué d'une désignation alphanumérique, indiquant les résultats combinés des évaluations de probabilité et de gravité. Les combinaisons respectives gravité/probabilité sont présentées dans la matrice d'évaluation des risques de sécurité (Figure 2-13).

2.14.10 La troisième étape du processus consiste à déterminer la tolérabilité des risques de sécurité. En premier lieu, il faut obtenir les indices dans la matrice d'évaluation des risques de sécurité. Par exemple, considérer une situation où la probabilité des risques de sécurité aura été évaluée comme occasionnelle (4) et où la gravité de ces risques aura été évaluée comme dangereuse (B). La combinaison de la probabilité et de la gravité (4B) est l'indice de risque de sécurité des conséquences.

Gravité	Signification	Valeur
Catastrophique	<ul style="list-style-type: none"> — Équipement détruit — Morts multiples 	A
Dangereux	<ul style="list-style-type: none"> — Importante réduction des marges de sécurité, détresse physique ou charge de travail telle qu'il n'est pas sûr que les opérateurs pourront accomplir leur tâche exactement ou complètement — Blessure grave — Dommage majeur à l'équipement 	B
Majeur	<ul style="list-style-type: none"> — Importante réduction des marges de sécurité, réduction de la capacité des opérateurs de faire face à des conditions de travail défavorables, du fait d'une augmentation de la charge de travail ou comme résultat de conditions compromettant leur efficacité — Incident grave — Blessures à des personnes 	C
Mineur	<ul style="list-style-type: none"> — Nuisance — Limites de fonctionnement — Application de procédures d'urgence — Incident mineur 	D
Négligeable	<ul style="list-style-type: none"> — Peu de conséquences 	E

Figure 2-12. Tableau de gravité des risques de sécurité

Probabilité du risque	Gravité du risque				
	Catastrophique A	Dangereux B	Majeur C	Mineur D	Négligeable E
Fréquent 5	5A	5B	5C	5D	5E
Occasionnel 4	4A	4B	4C	4D	4E
Éloigné 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extrêmement improbable 1	1A	1B	1C	1D	1E

Figure 2-13. Matrice d'évaluation d'un risque de sécurité

2.14.11 L'indice obtenu à partir de la matrice d'évaluation des risques de sécurité doit ensuite être exporté vers une matrice de tolérabilité des risques de sécurité (voir la Figure 2-14) qui décrit les critères de tolérabilité pour l'organisation considérée. En utilisant l'exemple ci-dessus, le critère pour un risque de sécurité évalué comme 4B entre dans la catégorie « inacceptable dans les circonstances existantes ». Dans ce cas, l'indice de risque de sécurité de la conséquence est inacceptable. L'organisation doit donc :

- a) prendre des mesures pour réduire l'exposition de l'organisation aux risques particuliers dont il s'agit, c'est-à-dire réduire la composante de probabilité de l'indice de risque ;
- b) prendre des mesures pour réduire la gravité des conséquences liées au danger, c'est-à-dire réduire la composante de gravité de l'indice de risque ; ou
- c) annuler l'opération si une atténuation n'est pas possible.

Note.— La pyramide inversée de la Figure 2-14 reflète un effort constant pour tirer l'indice de risque vers le SOMMET qui est à la base de la pyramide. La Figure 2-15 présente un exemple de matrice alternative de tolérabilité du risque de sécurité.

2.15 GESTION DES RISQUES DE SÉCURITÉ

2.15.1 La gestion des risques de sécurité englobe l'évaluation des risques de sécurité et leur atténuation. Son objectif est d'évaluer les risques associés aux dangers identifiés et de développer et mettre en œuvre des atténuations efficaces et appropriées. La gestion des risques de sécurité est donc un élément clé du processus de gestion de la sécurité, au niveau de l'État et au niveau du fournisseur de produits/services.

2.15.2 Les risques de sécurité sont évalués conceptuellement comme étant acceptables, tolérables ou intolérables. Les risques évalués comme tombant initialement dans la région intolérable sont inacceptables dans n'importe quelles circonstances. La probabilité et/ou la gravité des conséquences des dangers sont d'une ampleur telle, et le potentiel dommageable du danger pose une telle menace à la sécurité, qu'une action d'atténuation immédiate est nécessaire.

2.15.3 Les risques de sécurité évalués dans la région tolérable sont acceptables pourvu que les stratégies d'atténuation appropriées soient mises en œuvre par l'organisation. Un risque de sécurité initialement évalué comme intolérable pourra être atténué et ultérieurement déplacé dans la région tolérable pourvu que ces risques demeurent contrôlés par des stratégies d'atténuation appropriées. Dans les deux cas, une analyse coûts-avantages complémentaire pourra être effectuée si c'est jugé approprié. Voir plus de précisions au § 2.15.7.

2.15.4 Des risques de sécurité évalués initialement comme tombant dans la région acceptable sont acceptables tels quels et n'exigent aucune mesure pour amener ou maintenir la probabilité et/ou la gravité des conséquences de dangers sous contrôle organisationnel.

Documents/feuille de calcul de gestion des risques

2.15.5 Chaque activité d'atténuation de risques devra être documentée comme c'est nécessaire. Cela pourra être fait sur une feuille de calcul ou sur un tableau simple pour l'atténuation de risques qui ne concernent pas des opérations, processus ou systèmes complexes. Pour l'identification de dangers et l'atténuation de risques concernant des processus, systèmes ou opérations complexes, il pourra être nécessaire d'utiliser des logiciels sur mesure pour l'atténuation des risques, afin de faciliter le processus de documentation. Les documents remplis concernant l'atténuation des risques devraient être approuvés au niveau de gestion compétent. Voir à l'Appendice 2 un exemple de feuille de travail de base.

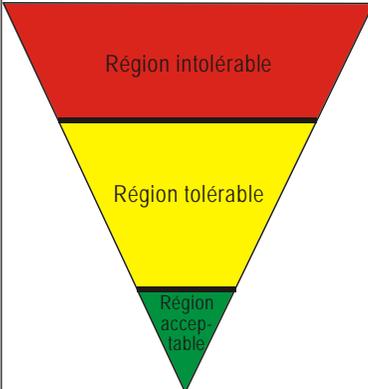
Description de la tolérabilité	Indice de risque évalué	Critères suggérés
 Région intolérable	5A, 5B, 5C, 4A, 4B, 3A	Inacceptable dans les circonstances existantes
Région tolérable	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Acceptable sur la base d'une atténuation de risque. Peut exiger une décision de la direction.
Région acceptable	3E, 2D, 2E, 1B, 1C, 1D, 1E	Acceptable

Figure 2-14. Matrice de tolérabilité des risques de sécurité

Plage d'indice de risque	Description	Mesures recommandées
5A, 5B, 5C, 4A, 4B, 3A	Risque élevé	Cesser les opérations ou les réduire promptement si nécessaire. Effectuer l'atténuation de risque prioritaire pour assurer que des contrôles préventifs supplémentaires ou améliorés soient mis en place pour ramener l'indice de risque à la plage de risque modéré à faible.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Risque modéré	Planifier l'exécution d'une évaluation de sécurité pour abaisser l'indice de risque à la plage basse, si viable.
3E, 2D, 2E, 1B, 1C, 1D, 1E	Risque faible	Acceptable tel quel. Aucune autre atténuation de risque requise.

Figure 2-15 Autre matrice de tolérabilité des risques de sécurité

Facteurs humains et gestion des risques

2.15.6 Étant donné que des PNS et SGS à maturité visent des facteurs aussi bien humains qu'organisationnels, un processus d'analyse spécifique est un élément de tout système de gestion des risques à maturité et efficace. Au cours de toute activité d'identification des dangers et d'atténuation des risques faisant intervenir des éléments humains, il faut s'assurer que les défenses existantes ou recommandées ont pris en considération les facteurs humains (HF). Au besoin, une analyse HF complémentaire pourra être effectuée pour appuyer l'activité/l'équipe particulière d'atténuation des risques. Une analyse HF apporte une compréhension de l'impact de l'erreur humaine sur la situation et contribue en

définitive au développement d'actions d'atténuation/correctives plus complètes et efficaces. Un modèle d'erreur humaine est la base du processus d'analyse ; il définit la relation entre performances et erreurs et catégorise les erreurs pour permettre que les dangers profonds soient plus aisément identifiés et mieux compris. Cette compréhension assure la réalisation adéquate d'une analyse des causes profondes. Les actions et les décisions individuelles considérées hors contexte peuvent apparaître comme des événements pratiquement aléatoires, échappant à l'attention voulue. Le comportement humain n'est pas nécessairement aléatoire. Il est habituellement conforme à un certain modèle et peut être analysé et bien compris. En définitive, cette importante perspective HF a pour résultat un processus d'atténuation plus complet et approfondi. Une analyse HF assure que pendant le processus d'atténuation des risques de l'organisation, lorsque des facteurs profonds, des facteurs contributifs ou des facteurs d'escalade sont identifiés, il est dûment tenu compte des facteurs humains et des impacts qui leur sont associés aux niveaux des circonstances, de la supervision et de l'organisation.

Analyse coûts-avantages (CBA)

2.15.7 L'analyse coûts-avantages ou coût-efficacité est normalement un processus indépendant de l'atténuation ou de l'évaluation des risques de sécurité. Elle est communément associée à un protocole de gestion de haut niveau, tel qu'une évaluation d'impact réglementaire ou un projet d'expansion des activités. Il peut y avoir cependant des situations où une évaluation de risque peut se situer à un niveau suffisamment élevé ou avoir un impact financier important. Dans de telles situations, un processus supplémentaire d'analyse CBA ou de coût-efficacité pour appuyer l'évaluation de risques peut se justifier. Ceci pour assurer que l'analyse coût-efficacité ou la justification de mesures d'atténuation ou de contrôles préventifs recommandés ait pris en considération les incidences financières qui s'y rattachent.

2.16 SPÉCIFICATIONS PRESCRIPTIVES ET SPÉCIFICATIONS FONDÉES SUR LES PERFORMANCES

Comprendre les spécifications fondées sur les performances

2.16.1 De plus en plus, au sein de la communauté de l'aviation, on a la conviction que la mise en œuvre efficace d'un programme national de sécurité (PNS) et d'un système de gestion de la sécurité (SGS) exige que l'approche prescriptive de la sécurité, actuellement existante, soit complétée par une approche fondée sur les performances. S'appuyant sur la collecte et l'analyse de données pertinentes, celle-ci est rationnelle sur le plan commercial tout en offrant un niveau de sécurité équivalent.

2.16.2 Un des objectifs d'un SGS est d'introduire des éléments supplémentaires fondés sur la performance pour un contrôle plus efficace des risques de sécurité. Dans un environnement réglementaire classique fondé sur la conformité, l'approche de la gestion de la sécurité est relativement rigide et prescriptive, les règlements relatifs à la sécurité étant utilisés comme contrôles administratifs. Un cadre réglementaire s'appuie sur des inspections et des audits pour assurer la conformité réglementaire.

2.16.3 Dans un contexte de sécurité amélioré, fondé sur les performances, certains éléments fondés sur les performances sont introduits au sein d'un cadre prescriptif. Ceci permettra que l'aspect « conformité » d'un règlement laisse de la place pour une performance plus souple, fondée sur le risque (et donc plus dynamique). En résultat, certains éléments dans les cadres SGS et PNS pourront être gérés selon une démarche de plus en plus fondée sur les performances plutôt que selon une approche purement prescriptive. Ces éléments fondés sur les performances relèvent des éléments d'assurance de la sécurité et de gestion des risques de sécurité des cadres respectifs.

2.16.4 Dans un cadre SGS/PNS, les éléments fondés sur les performances comprennent le processus de surveillance et de mesure des performances de sécurité au niveau de chaque fournisseur de produits ou de services,

aussi bien qu'au niveau de l'État. Cela permet que l'organisation choisisse ses propres indicateurs de surveillance de la sécurité et fixe des alertes et des objectifs pertinents pour son propre contexte, son historique de performances et ses attentes. Il n'est pas fixé d'indicateurs de sécurité prescrits ou de niveaux d'alerte ou de valeurs prescrits (obligatoires) selon cette attente SGS/PNS.

Conditions requises pour les spécifications fondées sur les performances

2.16.5 L'État et ses fournisseurs de produits et de services devraient avoir en place, respectivement, un PNS et un SGS. Une interface devra être en place pour que les instances de réglementation se mettent d'accord avec chacun des fournisseurs de produits et services sur leurs indicateurs de performance de sécurité en rapport avec le SGS et avec les objectifs et les réglages d'alerte connexes. Le réglementeur devra aussi avoir un processus pour une surveillance continue des performances de sécurité de chaque fournisseur de produits et services. Les nouveaux processus supplémentaires fondés sur les performances, introduits et dûment acceptés/approuvés par le réglementeur, devraient avoir des indicateurs de performances appropriés, mis au point pour surveiller de tels processus fondés sur les performances. De tels indicateurs, spécifiques à un processus, peuvent être considérés comme des indicateurs complémentaires aux indicateurs de performances de sécurité du SGS de niveau supérieur.

Niveau de sécurité de référence et niveau de sécurité équivalent

2.16.6 Le résultat, en matière de performances de sécurité, de l'introduction d'éléments fondés sur les performances au sein d'un cadre SGS, ou en complément d'un cadre SGS, ne devrait pas être plus mauvais que celui d'un cadre réglementaire existant, purement prescriptif. Pour évaluer une telle « équivalence » ou contrôler que cette équivalence est vraiment le cas, il devrait y avoir des indicateurs de sécurité pour surveiller l'issue générale des événements (occurrences de non-conformité) du système/processus concerné pour lequel l'élément fondé sur les performances aura été introduit. À titre d'exemple, le taux moyen d'incidents dans la FPFM (gestion de la planification du vol et du carburant) générale après l'introduction de dispositions fondées sur les performances ne devrait pas être plus mauvais que le taux d'incidents avant l'introduction de dispositions FPFM fondées sur les performances. Par un tel processus de comparaison, les performances « de référence » prémise en œuvre pourront être vérifiées par rapport aux performances post-mise en œuvre, pour voir si un niveau de performance « équivalent » a été maintenu. Si la performance post-mise en œuvre se révèle meilleure, alors un « meilleur » niveau de performance aura en fait été manifesté. S'il y a dégradation de la performance du système, le fournisseur de services devrait travailler conjointement avec le réglementeur pour vérifier les facteurs causaux et prendre les dispositions appropriées ; celles-ci pourront comprendre la modification de la spécification fondée sur les performances elle-même ou, au besoin, le rétablissement de spécifications prescriptives de base. Le § 2.16.7, ainsi que les Chapitres 4 et 5 de ce manuel, donnent plus de précisions sur la manière dont les performances du système peuvent être mesurées par des indicateurs de performance de sécurité.

Surveillance et mesure fondées sur les performances

2.16.7 La surveillance et la mesure d'un processus fondé sur les performances devraient se faire au moyen d'indicateurs appropriés de performances, de qualité ou de sécurité suivant en continu les performances de ce processus. Les paramètres pour un tel suivi de performances peuvent être des résultats d'occurrences, des écarts ou tous types d'événements reflétant le niveau de sécurité, de qualité ou de risque du processus. Un graphe de tendance des données devrait être utilisé pour suivre de tels résultats. Les occurrences résultantes devraient normalement être suivies comme taux d'occurrence plutôt que comme nombres absolus. Conjointement avec de tels indicateurs, il faudrait que soient fixés pour chaque indicateur, si c'est applicable, des niveaux d'alerte ainsi que des niveaux visés d'amélioration souhaitée. Ceux-ci serviront de marqueurs pour définir le taux d'occurrence anormal/inacceptable ainsi que le taux (d'amélioration) visé souhaité pour l'indicateur. Le réglage du niveau d'alerte servira effectivement de ligne

de démarcation entre la région d'établissement de tendance acceptable et la région inacceptable pour un indicateur de sécurité. Tant que le taux d'occurrence pour un processus n'a pas tendance à dépasser les critères fixés du niveau d'alerte, ou ne les dépasse pas, le nombre de ces occurrences est censé être acceptable (non anormal) pour cette période de surveillance. Par ailleurs, le but d'un niveau d'amélioration visé est de réaliser le niveau d'amélioration souhaité dans un certain délai ou dans une période de surveillance future définie. Avec de tels réglages définis d'alerte et d'objectif, il apparaît qu'un résultat de performance qualitatif/quantitatif peut être obtenu à la fin de toute période de surveillance donnée. Ceci pourra se faire en comptant le nombre de dépassements du niveau d'alerte et/ou le nombre d'objectifs atteints pour un certain indicateur et/ou un ensemble d'indicateurs de sécurité. Il sera question aux Chapitres 4 et 5, respectivement, des indicateurs de performances de sécurité et des méthodes de fixation d'objectifs d'alerte.

Supervision de spécifications fondées sur les performances

2.16.8 Contrairement aux audits de spécifications prescriptives, autonomes, l'évaluation d'un processus fondé sur les performances exigerait que l'évaluateur connaisse le contexte de ce processus/cet élément dans son cadre réglementaire général aussi bien que dans la complexité de l'organisation auditée. Il ne peut pas y avoir de critères simples, « *go/no-go* » ou réussite/échec, à appliquer. Un exemple serait l'acceptabilité d'un système de compte rendu de danger ou l'acceptabilité de niveaux cibles/niveaux d'alerte proposés pour un processus fondé sur les performances, ceci pouvant impliquer plus d'interaction, de surveillance, de négociation et de jugement objectif pour le responsable d'audit. Le niveau ou le degré de conformité ou de performances de tels éléments varierait aussi en fonction de la complexité du processus ou de l'opération auditée. Un exemple de performance ou de conformité d'un élément qui est sujet à une complexité de l'organisation ou du processus est le processus d'atténuation du risque. Un processus d'atténuation du risque pourrait comporter l'utilisation d'une feuille de calcul d'une page pour une tâche d'atelier qui est une opération simple d'un seul homme. Par contre, l'atténuation de risque pour un processus multidisciplinaire complexe (p. ex. opérations dans un espace aérien affecté par des éruptions volcaniques) peut exiger l'utilisation d'un logiciel d'atténuation de risque pour effectuer une évaluation de sécurité suffisamment complète pour être satisfaisante.

Appendice 1 au Chapitre 2

LISTE DE VÉRIFICATION POUR ÉVALUATION DE LA CULTURE DE SÉCURITÉ DE L'ORGANISATION (OSC)/ DU PROFIL DE RISQUE DE L'ORGANISATION (ORP) — EXPLOITANTS AÉRIENS

Note.— Cette liste de vérification pour évaluation OSC/ORP est seulement une illustration conceptuelle. Les 37 paramètres illustrés ne sont pas exhaustifs et sont applicables pour un exploitant aérien. Il serait nécessaire de les adapter pour l'évaluation d'autres types de prestataires de services. Les notes de résultats sont purement destinées à servir d'illustration. Cette évaluation OSC/ORP devrait être menée sur une base volontaire, les paramètres de culture/profil d'organisation ne relevant pas du domaine normal de la réglementation. Voir au Chapitre 2, § 2.6.19, une application suggérée pour un tel dispositif d'évaluation OSC/ORP.

Colonne de résultat. Dans le menu déroulant, sélectionner « 1 » (L1), « 2 » (L2), « 3 » (L3) ou « N/A » selon l'évaluation POI/PMI /AOC ORP Mar 12

2-App 1-1

Nom de l'organisation		Évalué par / date			
	Paramètre de risque d'organisation	Niveau/profil de risque			Résultat (Niveau #)
		Niveau 3 (le moins souhaitable)	Niveau 2 (moyen)	Niveau 1 (le plus souhaitable)	
1	Dirigeant responsable — propriété des fonctions de sécurité/qualité	Fonctions de sécurité/qualité inexistantes dans le mandat du dirigeant responsable	Mention négligeable ou indistincte des fonctions de sécurité/qualité dans le mandat du dirigeant responsable	Reddition de comptes pour questions de sécurité et qualité clairement traitée dans le mandat du dirigeant responsable	3
2	État financier de l'organisation	à définir	à définir	à définir	2
3	Âge moyen de la flotte	Plus de 12 ans	8 à moins de 12 ans	Moins de 8 ans	2
4	Note de performance du SGS	Année 2011 : 65 % à 75 %	76 % à 90 %	Plus de 90 %	3
5	Programme actif d'identification des dangers et d'évaluation de risque (HIRA)	Pas de programme HIRA actif en place	Programme HIRA en place. Réalisation ou examen de 1 à 3 projets d'évaluation de risque (pour 100 employés opérationnels) dans les 12 derniers mois.	Programme HIRA en place pour toutes les grandes questions opérationnelles. Réalisation de plus de 3 projets d'évaluation de risque (pour 200 employés opérationnels) pour tous les domaines opérationnels au cours des 12 derniers mois.	2
6	Horaires ou calendriers exigeants du personnel de conduite (nombre d'incidents liés à la limitation des heures de vol ?)	à définir	à définir	à définir	2

	Paramètre de risque d'organisation	Niveau/profil de risque			Résultat (Niveau #)
		Niveau 3 (le moins souhaitable)	Niveau 2 (moyen)	Niveau 1 (le plus souhaitable)	
7	Ratio du personnel interne de contrôle de sécurité plus qualité au personnel opérationnel	1: plus de 20	1:15 à 20	1: moins de 15	3
8	Vol sur flotte mixte (MFF) (pourcentage de pilotes en MFF — un pourcentage plus élevé est moins souhaitable)	à définir	à définir	à définir	1
9	Routes EDTO (pourcentage de secteurs EDTO exploités) (un pourcentage plus élevé est moins souhaitable)	à définir	à définir	à définir	2
10	Durée EDTO (une plus grande durée est moins souhaitable)	à définir	à définir	à définir	2
11	Expérience dans la compagnie (années de travail)	Moins de 5 ans	5 à 10 ans	Plus de 10 ans	3
12	Rotation du personnel combinée pour le dirigeant responsable, le gestionnaire sécurité et le gestionnaire qualité au cours des 36 derniers mois	3 ou plus	2	1 ou rien	2
13	Expérience et qualifications du dirigeant responsable (à la date de l'évaluation)	Moins de 3 ans d'expérience en aviation et pas de qualification technique	Plus de 3 ans d'expérience en aviation ou qualifications techniques.	Plus de 3 ans d'expérience en aviation et qualifications techniques en aviation	3
14	Expérience et qualifications du gestionnaire sécurité (SM)	Moins de 5 ans d'expérience en sécurité/qualité de l'aviation civile ou pas de qualification technique en aviation	Plus de 5 ans d'expérience en sécurité/qualité de l'aviation civile et qualifications techniques en aviation	Plus de 15 ans d'expérience en sécurité/qualité de l'aviation civile et qualifications techniques en aviation	2
15	Expérience et qualifications du gestionnaire qualité	Moins de 5 ans d'expérience QC/QA en aviation civile et qualifications techniques en aviation	Plus de 5 ans d'expérience QC/QA en aviation civile et qualifications techniques en aviation	Plus de 15 ans d'expérience QC/QA en aviation civile et qualifications techniques en aviation	1
16	Personnel de gestion sécurité/qualité (QM/SM) à portefeuille multiple	Le personnel SM ou QM occupe simultanément d'autres postes de cadre dans l'organisation ou à l'extérieur	Le mandat du personnel SM ou QM comprend d'autres fonctions ne concernant pas directement la sécurité/qualité, p. ex. IT, administration, formation	Le personnel SM ou QM n'occupe pas simultanément d'autres postes de cadre dans l'organisation ou à l'extérieur et son mandat n'inclut pas d'autres fonctions ne concernant pas directement la qualité/la sécurité	2
17	Multiplicité des types d'aéronefs	Plus de 4 types d'aéronefs	3 ou 4 types d'aéronefs	Moins de 3 types d'aéronefs	1

	<i>Paramètre de risque d'organisation</i>	<i>Niveau/profil de risque</i>			<i>Résultat (Niveau #)</i>
		<i>Niveau 3 (le moins souhaitable)</i>	<i>Niveau 2 (moyen)</i>	<i>Niveau 1 (le plus souhaitable)</i>	
18	Taux d'incidents pouvant/devant faire l'objet d'un compte rendu pour la flotte combinée (par 1 000 FH) pour les 24 derniers mois	à définir	à définir	à définir	2
19	Réservé				
20	Taux IFSD des moteurs de la flotte combinée par 1 000 FH	à définir	à définir	à définir	2
21	Taux moyen d'applications MEL pour la flotte (par 1000 FH)	Plus de 30 applications MEL par 1 000 FH	10 à 30 applications MEL par 1 000 FH	Moins de 10 applications MEL par 1 000 FH	2
22	Taux de demande de concession technique interne	3 concessions par aéronef par an	Plus de 1 concession par aéronef par an	Moins de 1 concession par aéronef par an	2
23	Taux de demande de concession technique par l'AAC.	Plus de 1 concession par aéronef par an	Plus de 0,5 concession par aéronef par an	Moins de 0,5 concession par aéronef par an	2
24	Structure de l'obligation de rendre compte en matière de sécurité	La fonction/le bureau/le gestionnaire chargé de la gestion de la sécurité a l'obligation de rendre compte ou est subordonné à certaines fonctions opérationnelles	La fonction/le bureau/le gestionnaire chargé de la gestion de la sécurité a l'obligation de rendre compte à la haute direction et est indépendant de toutes fonctions opérationnelles	La fonction/le bureau/le gestionnaire chargé de la gestion de la sécurité a l'obligation de rendre compte au CEO et relève directement de lui	3
25	Structure de l'obligation de rendre compte en matière de qualité	La fonction/le bureau/le gestionnaire chargé de la gestion de la qualité a l'obligation de rendre compte ou est subordonné à des fonctions non liées à la qualité/sécurité	La fonction/le bureau/le gestionnaire chargé de la gestion de la qualité a l'obligation de rendre compte à la haute direction et est indépendant de toutes fonctions opérationnelles	La fonction/le bureau/le gestionnaire chargé de la gestion de la qualité a l'obligation de rendre compte au CEO et relève directement de lui	3
26	Taux de constatations d'audit de l'organisation AOC par l'AAC (constatations de niveaux 1 et 2 seulement, observations exclues) au cours des 24 derniers mois	Toute constatation de niveau 1 ou plus de 5 constatations par audit par aéronef	Plus de 1 constatation par audit par aéronef	Moins de 1 constatation par audit par aéronef	2
27	Taux de constatations LSI par l'AAC (constatations de niveaux 1 et 2 seulement, observations exclues) au cours des 24 derniers mois	Toute constatation de niveau 1 ou plus de 3 par audit par station de maintenance en ligne	Plus de 0,5 constatation par audit par station de maintenance en ligne	Moins de 0,5 constatation par audit par station de maintenance en ligne	2

	Paramètre de risque d'organisation	Niveau/profil de risque			Résultat (Niveau #)
		Niveau 3 (le moins souhaitable)	Niveau 2 (moyen)	Niveau 1 (le plus souhaitable)	
28	Politique sur la durée de vie des composantes (articles durables/ /LRU) <i>soft</i> /CM/ <i>hard</i> au-delà des spécifications obligatoires ou des exigences du MPD	Pas de politique de contrôle de la durée de vie des composantes (<i>hard</i> / <i>soft</i>) au-delà des spécifications obligatoires ou des exigences du MPD	Politique et procédures <i>hard</i> de contrôle de durée de vie des composantes actives. Au moins 5 à 10 % de tous les articles durables (énumérés dans MPD/AMS) de commande du vol et des moteurs (au-delà des spécifications obligatoires du MPD) ont eu une durée de vie <i>soft</i> ou <i>hard</i> .	Politique et procédures <i>hard</i> de contrôle de durée de vie des composantes actives. Plus de 10 % de tous les articles durables (énumérés dans MPD/AMS) de commande du vol et des moteurs (au-delà des spécifications obligatoires du MPD) ont eu une durée de vie <i>soft</i> ou <i>hard</i> .	3
29	Portée des investigations QA et du processus MEDA	Processus d'investigation QA interne appliqué aux incidents à compte rendu obligatoire seulement	Processus d'investigation QA interne pour tous les incidents dont il est rendu compte	Processus d'investigation QA interne pour tous les incidents dont il est rendu compte + MEDA (ou processus équivalent)	
30	Existence d'un programme de protection de l'environnement	Inexistant	Participation isolée à un programme de protection de l'environnement	Programme habituel et engagement et participation réguliers dans un programme de protection de l'environnement en aviation	3
31	Existence d'un programme d'inspection spécial basé sur des publications d'un service OEM non obligatoire	Programme d'inspection spécial pour SB liés aux AD seulement	Programme d'inspection spécial pour AD ainsi que SB d'alerte seulement	Programme d'inspection spécial pour AD, SB d'alerte ainsi que publications courantes du service OEM	2
32	Contrôle de la gestion technique de la flotte	Entièrement sous-traité à un organisme extérieur (FTM + ITM)	Partiellement sous-traité à un organisme extérieur	Gestion interne par un organisme AOC	2
33	Emploi de personnel technique contractuel	Plus de 15 % de personnel contractuel (d'un autre organisme) pour fonctions internes d'ingénierie/techniques	5 à 15 % de personnel contractuel (d'un autre organisme) pour fonctions internes d'ingénierie/techniques	Moins de 5 % de personnel contractuel (d'un autre organisme) pour fonctions internes d'ingénierie/techniques	2
34	Certification d'inspection en transit par des pilotes, techniciens ou AME	Pratique la certification en transit par des pilotes au lieu de technicien d'ingénierie/AME qualifié	Pratique la certification d'inspection en transit par des techniciens (qualification limitée) au lieu d'AME	Pratique la certification d'inspection en transit seulement par des AME (entièrement qualifiés sur type)	3
35	Système de compte rendu de danger	Pas de système en place	Un système de compte rendu volontaire de danger est en place	Un système de compte rendu volontaire de danger est en place. Il y a aussi une procédure pour l'identification des dangers conjointement avec un processus d'enquête sur incidents.	2

	Paramètre de risque d'organisation	Niveau/profil de risque			Résultat (Niveau #)
		Niveau 3 (le moins souhaitable)	Niveau 2 (moyen)	Niveau 1 (le plus souhaitable)	
36	Procédures de compte rendu d'incidents, d'investigations et de mesures correctives	Pas de procédures documentées de compte rendu d'incidents, d'investigations ou de mesures correctives	Procédures documentées de compte rendu d'incidents, d'investigations et de mesures correctives	Procédures documentées de compte rendu d'incidents, d'investigations et de mesures correctives, acceptées par l'AAC	2
37	Gestion des dossiers techniques, des fournitures techniques et de la planification de la flotte	Sous-traite complètement à un organisme extérieur la gestion des dossiers techniques, des fournitures techniques et de la planification de la flotte	Sous-traite à un organisme extérieur la gestion de dossiers techniques, de fournitures techniques ou de la planification de la flotte	Gestion interne (au sein de l'organisme) des dossiers techniques, des fournitures techniques et de la planification de la flotte	3

	Total partiel
Niveau 3	11
Niveau 2	21
Niveau 1	3
N/A	0
Nombre total de questions	37

Résultat de l'évaluation	
Nombre total de points	Catégorie ORP
78	D

Catégorisation ORP	
Note totale	Catégorie ORP
35–49	A (souhaitable)
50–63	B
64–77	C
78–91	D
92–105	E (le moins souhaitable)

Notes.—

1. Descriptions de critères/chiffres de niveau de risque données à des fins d'illustration seulement, sous réserve d'adaptation et de validation des chiffres réels à utiliser.
2. La liste de vérification devra être adaptée pour les AMO, aéroports et fournisseurs de services ATS.
3. Points à attribuer pour chaque paramètre évalué — à savoir 1, 2 ou 3 pour niveaux 1, 2 et 3 respectivement.
4. Cette évaluation de liste de vérification OSC/ORP peut être effectuée selon un calendrier prévu (par exemple pendant un audit de l'organisation) par l'inspecteur/vérificateur désigné. Celui-ci pourrait devoir se mettre en rapport avec le prestataire de services pour obtenir certaines des données nécessaires.
5. Ce processus d'évaluation OSC/ORP pourrait n'être pas obligatoire, considérant les paramètres qui sont en dehors du domaine normal de la réglementation, p. ex. taux de rotation du personnel. Il pourra être administré sur une base de participation complémentaire/volontaire.
6. Noter le nombre total de points et la catégorie ORP correspondante (Cat A à E). Les résultats devraient être communiqués à l'organisation évaluée.
7. Les résultats de cette évaluation OSC/ORP pourront être corrélés avec les constatations d'autres programmes réglementaires d'inspection/d'audit pour identifier les domaines (organisations) à propos desquels les préoccupations ou les besoins sont plus grands, selon les exigences de l'élément 3.3 du PNS. Autrement, la notification à chaque organisme des résultats de l'ORP pourrait suffire comme mécanisme pour encourager une évolution du comportement organisationnel (culture de la sécurité) vers la catégorie souhaitable, s'il y a lieu.

Appendice 2 au Chapitre 2

EXEMPLE DE FEUILLE DE CALCUL D'ATTÉNUATION D'UN RISQUE DE SÉCURITÉ

Note.— Pour faciliter la gestion des feuilles de calcul, il est préférable d'utiliser une feuille de calcul séparée pour chaque combinaison différente de Danger>Événement dangereux>Conséquence ultime.

Tableau 2-A2-1. Danger et conséquences

Opération/processus :	Décrire le processus/l'opération/l'équipement/le système soumis à cette activité HIRM.
Danger (H) :	S'il y a plus d'un danger dans l'opération/le processus, utiliser une feuille de calcul séparée pour chaque danger.
Événement dangereux (UE) :	S'il y a plus d'un UE pour le danger, utiliser une feuille de calcul séparée pour chaque combinaison UE-UC.
Conséquence ultime (UC) :	S'il y a plus d'une UC pour le danger, utiliser une feuille de calcul séparée pour chaque UC.

Tableau 2-A2-2. Indice de risque et tolérabilité des conséquences/UE (voir Supplément 1)

	Tolérabilité actuelle du risque (compte tenu de tout PC/RM/EC existant)			Indice de risque et tolérabilité résultants (compte tenu de tout PC/RM/EC nouveau)		
	Gravité	Probabilité	Tolérabilité	Gravité	Probabilité	Tolérabilité
Événement dangereux						
Conséquence ultime						

Tableau 2-A2-3. Atténuation de risque

Danger (H)	PC	EF	EC		RM	EF	EC	
H	PC1 (Existant)	EF (Existant)	EC1 (Existant)	UE	RM1	EF (à RM1)	EC (à EF)	UC
			EC2 (Nouveau)					
	PC2 (Existant)	EF1 (Nouveau)	EC (Nouveau)		RM2	EF (à RM2)	EC (à EF)	
			EC (Nouveau)					
	PC3 (Nouveau)	EF (Nouveau)	EC (Nouveau)		RM3	EF (à RM3)	EC (à EF)	
			EC (Nouveau)					

Notes explicatives.—

1. *Opération/processus (Tableau 2-A2-1)*. Description de l'opération ou du processus soumis à cette activité d'atténuation de danger/risque.
2. *Danger (H)*. Condition ou situation indésirable pouvant mener à un ou des événements ou occurrences dangereuses. Le terme « menace » (p. ex. TEM) est parfois employé au lieu de « danger ».
3. *Événement dangereux (UE)*. Événement dangereux intermédiaire possible avant toute conséquence ultime, accident ou résultat le plus crédible. L'identification d'un événement dangereux est applicable seulement lorsqu'il est nécessaire de distinguer et d'établir des mesures d'atténuation en aval et en amont d'un tel événement intermédiaire (avant la conséquence ultime/l'accident) (p. ex. « événement de surchauffe » avant une « défaillance moteur »). Si cet état intermédiaire UE n'est pas applicable pour une opération particulière, il peut être exclu s'il y a lieu.
4. *Conséquence ultime (UC)*. Le résultat le plus crédible, événement ultime ou accident.
5. *Contrôle préventif (PC)*. Mesure d'atténuation/mécanisme/défense pour bloquer ou empêcher l'escalade d'un danger/d'une menace en un événement dangereux ou une conséquence ultime.
6. *Facteur d'escalade (EF)*. Condition latente/facteur latent possible pouvant affaiblir l'efficacité d'un contrôle préventif ou d'une mesure de rétablissement. Utiliser s'il y a lieu seulement. Il est possible qu'un facteur d'escalade puisse être désigné parfois comme une « menace ».
7. *Contrôle d'escalade (EC)*. Mesure/mécanisme d'atténuation pour bloquer ou empêcher qu'un facteur d'escalade compromette ou affaiblisse un contrôle préventif (ou une mesure de rétablissement). Utiliser seulement s'il y a lieu.
8. *Indice de risque actuel et tolérabilité*. Une mesure d'atténuation du risque (Tableau 2-A2-3) est applicable lorsqu'un niveau de tolérabilité actuel inacceptable d'un événement dangereux ou d'une conséquence ultime est identifié dans le Tableau 2-A2-2. L'indice de risque actuel et la tolérabilité tiendront compte des mesures de contrôle préventif existantes, s'il y a lieu.
9. *Indice de risque résultant et tolérabilité*. L'indice de risque résultant et la tolérabilité sont basés sur les mesures de contrôle préventif existantes, s'il y en a, combinées avec les nouvelles mesures de contrôle préventif/contrôle d'escalade/rétablissement mises en place comme résultat de l'activité d'atténuation de risque effectuée.

Supplément à l'Appendice 2. Tableaux types de gravité, de probabilité, d'indice de risque et de tolérabilité

Tableau Supp-1. Tableau de gravité (de base)

Niveau	Descripteur	<i>Description de la gravité (adapter selon la nature du produit ou les opérations du prestataire de services)</i>
1	Insignifiant	Sans importance pour la sécurité opérationnelle en rapport avec les aéronefs
2	Mineur	Dégrade ou affecte les procédures opérationnelles ou la performance normales des aéronefs
3	Modéré	Perte partielle de systèmes de bord importants/majeurs ou aboutit à une application anormale de procédures de vol
4	Majeur	Défaillance complète de systèmes de bord importants/majeurs ou aboutit à l'application d'urgence de procédures de vol
5	Catastrophique	Perte d'aéronef ou de vies humaines

Tableau Supp-2. Tableau de gravité (autre)

Niveau	Descripteur	<i>Description de la gravité (adapter selon la nature du produit ou les opérations du prestataire de services)</i>					
		<i>Sécurité de l'aéronef</i>	<i>Blessures</i>	<i>Dommmages aux biens</i>	<i>Perte potentielle de revenus</i>	<i>Dommmages à l'environnement</i>	<i>Dommmage à la réputation de l'entreprise</i>
1	Insignifiante	Sans importance pour la sécurité opérationnelle en rapport avec les aéronefs	Pas de blessures	Pas de dommages	Pas de pertes de revenus	Sans effet	Pas d'incidences
2	Mineure	Dégrade ou affecte les procédures opérationnelles ou la performance normales des aéronefs	Blessures mineures	Dommmages mineurs Moins de __ \$	Perte mineure Moins de __ \$	Effet mineur	Incidence locale limitée
3	Modérée	Perte partielle de systèmes de bord importants/majeurs ou mène à l'application de procédures de vol anormales	Blessure grave	Dommmages substantiels Moins de __ \$	Perte substantielle Moins de __ \$	Effet contenu	Incidence régionale
4	Majeure	Panne complète de systèmes de bord importants/majeurs ou aboutit à l'application d'urgence de procédures de vol	Un mort	Dommmages majeurs Moins de __ \$	Perte majeure Moins de __ \$	Effet majeur	Incidence nationale
5	Catastrophique	Perte de l'aéronef/la coque	Plusieurs morts	Dommmages catastrophiques Plus de __ \$	Perte massive Plus de __ \$	Effet massif	Incidence internationale

Note.— Employer le plus haut niveau de gravité obtenu pour calculer l'indice de risque dans le tableau de matrice d'indice de risque.

Tableau Supp-3. Tableau de probabilité

Niveau	Descripteur	Description de la probabilité
A	Certaine/fréquente	Devrait se produire dans la plupart des circonstances
B	Probable/occasionnelle	Se produira probablement à un moment donné
C	Possible/éloignée	Pourrait se produire à un moment donné
D	Peu probable/improbable	Pourrait peut-être se produire à un moment donné
E	Exceptionnelle	Pourrait se produire seulement dans des circonstances exceptionnelles

Tableau Supp-4. Matrice d'indice de risque (gravité x probabilité)

Probabilité	Gravité				
	1. Insignifiante	2. Mineure	3. Modérée	4. Majeure	5. Catastrophique
A. Certaine/fréquente	Modérée(1A)	Modérée (2A)	Élevée (3A)	Extrême (4A)	Extrême (5A)
B. Probable/occasionnelle	Basse (1B)	Modérée (2B)	Modérée(3B)	Élevée (4B)	Extrême (5B)
C. Possible/éloignée	Basse (1C)	Basse (2C)	Modérée (3C)	Modérée (4C)	Élevée (5C)
D. Peu probable/improbable	Négligeable (1D)	Basse (2D)	Basse (3D)	Modérée (4D)	Modérée (5D)
E. Exceptionnelle	Négligeable (1E)	Négligeable (2E)	Basse (3E)	Basse (4E)	Modérée (5E)

Tableau Supp-5. Tableau d'acceptabilité (tolérabilité) du risque

Indice de risque	Tolérabilité	Mesures requises (adapter comme il convient)
5A, 5B, 4A	Risque extrême	Arrêter immédiatement l'opération ou le processus. Inacceptable dans les circonstances existantes. Ne permettre aucune opération à moins que des mesures de contrôle suffisantes aient été prises pour ramener le risque à un niveau acceptable. Approbation de la haute direction requise.
5C, 4B, 3A	Risque élevé	Prudence. Veiller à ce que l'évaluation du risque ait été effectuée de façon satisfaisante et à ce que les contrôles préventifs déclarés soient en place. Approbation de l'évaluation du risque par des cadres supérieurs avant le commencement de l'opération ou du processus.
1A, 2A, 2B, 3B, 3C, 4C, 4D, 5D, 5E	Risque modéré	Effectuer ou revoir l'atténuation du risque selon les besoins. Approbation de l'évaluation du risque au niveau du service.
1B, 1C, 2C, 2D, 3D, 3E, 4E	Risque faible	Atténuation du risque ou examen facultatif.
1D, 1E, 2E	Risque négligeable	Acceptable tel quel. Une atténuation du risque n'est pas nécessaire.

Appendice 3 au Chapitre 2

ILLUSTRATION D'UNE PROCÉDURE DE PRIORISATION DES DANGERS

	<i>Option 1 (de base)</i>	<i>Option 2 (avancée)</i>																
Critères	Priorisation en rapport avec la catégorie de pire conséquence possible du danger (gravité de l'incident)	Priorisation en rapport avec la catégorie d'indice de risque (gravité et probabilité) de la pire conséquence possible du danger.																
Méthodologie	<p>a) projeter la pire conséquence possible du danger ;</p> <p>b) projeter la classification d'occurrence probable de cette conséquence (c.-à-d. sera-t-elle considérée comme étant un accident, un incident grave ou un incident ?) ;</p> <p>c) conclure que la priorisation du danger est donc :</p> <table border="1" data-bbox="381 1094 867 1274"> <thead> <tr> <th><i>Conséquence projetée</i></th> <th><i>Niveau de danger</i></th> </tr> </thead> <tbody> <tr> <td>Accident</td> <td>Niveau 1</td> </tr> <tr> <td>Incident grave</td> <td>Niveau 2</td> </tr> <tr> <td>Incident</td> <td>Niveau 3</td> </tr> </tbody> </table>	<i>Conséquence projetée</i>	<i>Niveau de danger</i>	Accident	Niveau 1	Incident grave	Niveau 2	Incident	Niveau 3	<p>a) projeter le numéro d'indice de risque r (basé sur la matrice pertinente de gravité et de probabilité) de la pire conséquence possible du danger (voir la Figure 2-13 de ce chapitre) ;</p> <p>b) en se référant à la matrice de tolérabilité connexe, déterminer la catégorie de tolérabilité de l'indice de risque (c.-à-d. intolérable, tolérable ou acceptable) ou une terminologie/catégorisation équivalente ;</p> <p>c) conclure que la priorisation du danger est donc :</p> <table border="1" data-bbox="922 1222 1424 1415"> <thead> <tr> <th><i>Indice de risque projeté</i></th> <th><i>Niveau de danger</i></th> </tr> </thead> <tbody> <tr> <td>Intolérable/Risque élevé</td> <td>Niveau 1</td> </tr> <tr> <td>Tolérable/Risque modéré</td> <td>Niveau 2</td> </tr> <tr> <td>Acceptable/Risque bas</td> <td>Niveau 3</td> </tr> </tbody> </table>	<i>Indice de risque projeté</i>	<i>Niveau de danger</i>	Intolérable/Risque élevé	Niveau 1	Tolérable/Risque modéré	Niveau 2	Acceptable/Risque bas	Niveau 3
<i>Conséquence projetée</i>	<i>Niveau de danger</i>																	
Accident	Niveau 1																	
Incident grave	Niveau 2																	
Incident	Niveau 3																	
<i>Indice de risque projeté</i>	<i>Niveau de danger</i>																	
Intolérable/Risque élevé	Niveau 1																	
Tolérable/Risque modéré	Niveau 2																	
Acceptable/Risque bas	Niveau 3																	
Observations	L'option 1 prend en considération seulement la gravité de la conséquence projetée du danger.	L'option 2 prend en considération la gravité et la probabilité de la conséquence projetée du danger — critère plus complet que l'option 1.																

Note.— D'un point de vue pratique, l'option 1 est plus viable que l'option 2 aux fins d'un système de priorisation plus simple. Le but d'un tel système est de faciliter le tri et la priorisation des dangers pour des mesures d'atténuation de risque.

Une fois que chaque danger aura été priorisé, il apparaîtra que les dangers pourront être triés comme dangers de niveau 1, niveau 2 et niveau 3. La priorité ou l'attention pour l'atténuation du risque pourra ensuite être attribuée selon le niveau (1, 2 ou 3), comme il convient.

Chapitre 3

SARP DE L'OACI RELATIVES À LA GESTION DE LA SÉCURITÉ

3.1 INTRODUCTION

3.1.1 Le présent chapitre donne un aperçu des normes et pratiques recommandées (SARP) relatives à la gestion de la sécurité, initialement adoptées dans l'Annexe 1 — *Licences du personnel*, l'Annexe 6 — *Exploitation technique des aéronefs*, l'Annexe 8 — *Navigabilité des aéronefs*, l'Annexe 11 — *Services de la circulation aérienne*, l'Annexe 13 — *Enquêtes sur les accidents et incidents d'aviation* et l'Annexe 14 — *Aérodromes*. Ce chapitre contient aussi des renseignements sur la nouvelle Annexe 19 — *Gestion de la sécurité*, qui traite des responsabilités et des processus de gestion de la sécurité et regroupe les dispositions générales en matière de gestion de la sécurité.

3.1.2 Les SARP de l'OACI relatives à la gestion de la sécurité apportent les spécifications de haut niveau que les États doivent mettre en œuvre pour s'acquitter de leurs responsabilités de gestion de la sécurité en rapport avec, ou pour soutenir directement, la sécurité d'exploitation des aéronefs. Ces dispositions s'adressent à deux groupes de destinataires : États et prestataires de services. Dans le contexte de la gestion de la sécurité, le terme « prestataire de services » désigne toute organisation tenue de mettre en œuvre un système de gestion de la sécurité (SGS) selon le cadre SGS de l'OACI. Les prestataires de services de sécurité, dans ce contexte, comprennent :

- a) les organismes de formation agréés qui sont exposés à des risques de sécurité pendant la prestation de leurs services ;
- b) les exploitants d'aéronefs et d'hélicoptères autorisés à effectuer des vols internationaux de transport commercial ;
- c) les organismes de maintenance agréés qui fournissent des services à des exploitants d'avions ou d'hélicoptères engagés dans le transport aérien commercial international ;
- d) les organismes responsables de la conception de type et/ou de la construction d'aéronefs ;
- e) les fournisseurs de services de la circulation aérienne ;
- f) les exploitants d'aérodromes certifiés.

3.1.3 Les SARP de l'OACI relatives à la gestion de la sécurité exigent aussi qu'un niveau de sécurité acceptable soit établi par les États, comme défini par leurs objectifs de performance de sécurité et leurs indicateurs de performance de sécurité. Les Chapitres 4 et 5, respectivement, donnent plus de précisions sur ces deux sujets.

3.2 SPÉCIFICATIONS RELATIVES À LA GESTION DE LA SÉCURITÉ PAR LES ÉTATS

3.2.1 Les spécifications relatives à la gestion de la sécurité par les États portent sur les performances, le personnel et les processus, sous la responsabilité directe des États, qui sont nécessaires pour la sécurité du transport aérien. Elles incluent l'établissement et la tenue à jour d'un programme national de sécurité (PNS), la collecte, l'analyse et l'échange de données sur la sécurité et la protection des renseignements relatifs à la sécurité.

3.2.2 Un PNS exige des fonctions spécifiques exercées par les États, notamment l'application d'une législation, de règlements, de politiques et de directives à l'appui de la fourniture sûre et efficace de produits et services d'aviation sous son autorité. Pour l'établissement et la tenue à jour du PNS, l'OACI a élaboré un cadre qui comprend, au minimum, les quatre composants suivants, contenant 11 éléments qui les sous-tendent :

- a) politique et objectifs de l'État en matière de sécurité ;
- b) gestion des risques de sécurité par l'État ;
- c) assurance de la sécurité par l'État ;
- d) promotion de la sécurité par l'État.

Le Tableau 3-1 résume les références aux spécifications de l'État relatives à la gestion de la sécurité et au cadre PNS, tels qu'adoptés initialement dans les Annexes à la Convention relative à l'aviation civile internationale. On trouvera au Chapitre 4 de plus amples indications sur les spécifications relatives au PNS, le cadre PNS et le niveau de sécurité acceptable.

3.3 SPÉCIFICATIONS RELATIVES À LA GESTION DE LA SÉCURITÉ PAR LES PRESTATAIRES DE SERVICES

3.3.1 Les SARP de l'OACI comprennent aussi des spécifications relatives à la mise en œuvre d'un SGS par les prestataires de services et les exploitants d'aviation générale comme élément du PNS de chaque État. Le SGS prévoit les moyens d'identifier les dangers pour la sécurité, de mettre en œuvre des mesures de réduction des risques de sécurité, de surveiller les performances de sécurité et de réaliser une amélioration continue des performances de sécurité.

3.3.2 Un cadre SGS exige des activités et des processus spécifiques qui doivent être effectués par les prestataires de services d'aviation. Le cadre SGS de l'OACI comprend les quatre composants suivants, ainsi que 12 éléments qui les sous-tendent :

- a) politiques et objectifs en matière de sécurité ;
- b) gestion des risques de sécurité ;
- c) assurance de la sécurité ;
- d) promotion de la sécurité.

3.3.3 Les exploitants d'avions lourds ou d'avions à turboréacteurs de l'aviation générale Internationale, décrits dans l'Annexe 6, Partie II, Section III, établiront et tiendront à jour un SGS approprié à la taille et à la complexité des opérations, qui devrait inclure au minimum :

- a) un processus pour identifier les dangers réels ou potentiels, et évaluer les risques y associés ;
- b) un processus pour élaborer et mettre en œuvre les mesures correctives nécessaires pour maintenir un niveau de sécurité acceptable ;
- c) des dispositions pour la surveillance continue et l'évaluation régulière du caractère approprié et efficace des activités de gestion de la sécurité ;

Tableau 3-1. Sommaire de références aux spécifications des États relatives à la gestion de la sécurité et au cadre PNS initialement adoptées dans les Annexes à la Convention

<i>Source</i>		<i>Sujet</i>
<i>Annexe</i>	<i>Disposition</i>	
1 6, Parties I, II et III 8 11 13 14, Volume I	Définitions	Programme national de sécurité
6, Partie I	3.3.1 et 8.7.3.1	Établissement du PNS
6, Partie III	1.3.1	
8	5.1	
11	2.27.1	
13	3.2	
14, Volume I	1.5.1	
6, Partie I	3.3.2 et 8.7.3.2	Niveau acceptable du concept de performance de sécurité
6, Partie III	1.3.2	
8	5.2	
11	2.27.2	
14, Volume I	1.5.2	
13	5.12	Protection des dossiers sur les accidents et incidents
13	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.9	Collecte, analyse et échange de données sur la sécurité
1	Supplément C	Cadre PNS — composants et éléments
6, Partie I	Supplément I	
6, Partie III	Supplément I	
8	Supplément à la Partie II	
11	Supplément D	
13	Supplément F	
14	Supplément C	
13	Supplément E	Orientations juridiques relatives à la protection des renseignements provenant des systèmes de collecte et de traitement de données sur la sécurité

3.3.4 Le Tableau 3-2 présente un sommaire de références aux spécifications relatives à la gestion de la sécurité pour prestataires de services et exploitants d'aviation générale, y compris le cadre SGS, comme initialement adopté dans les Annexes à la Convention relative à l'aviation civile internationale. Le Chapitre 5 contient de plus amples éléments indicatifs concernant les spécifications pour les prestataires de services et le cadre SGS.

Tableau 3-2. Sommaire de références aux spécifications relatives à la gestion de la sécurité pour prestataires de services et exploitants d'aviation générale, y compris le cadre PNS, initialement adoptées dans les Annexes à la Convention

<i>Source</i>		<i>Sujet</i>
<i>Annexe</i>	<i>Disposition</i>	
1 6, Parties I, II et III 8 11 13 14, Volume I	Définitions	Système de gestion de la sécurité
1	Appendice 2, 4.1 et 4.2	Spécifications du SGS pour organismes de formation agréés
6, Partie I	3.3.3, 3.3.4, 8.7.3.3 et 8.7.3.4	Spécifications du SGS pour exploitants d'aéronefs et organismes de maintenance
6, Partie II	Section 3, 3.3.2.1 et 3.3.2.2	Spécifications du SGS pour avions engagés dans l'aviation générale internationale
6, Partie III	1.3.3 et 1.3.4	Spécifications du SGS pour exploitants d'hélicoptères
8	5.3 et 5.4	Spécifications du SGS pour organismes responsables de la conception de type et de la construction d'aéronefs (applicables à compter du 14 novembre 2013)
11	2.27.3 et 2.27.4	Spécifications du SGS pour les prestataires de services de la circulation aérienne
14, Volume I	1.5.3 et 1.5.4	Spécifications du SGS pour les exploitants d'aérodromes certifiés
1	Appendice 4	Cadre SGS
6, Partie I	Appendice 7	
6, Partie III	Appendice 4	
11	Appendice 6	
14, Volume I	Appendice 7	

3.4 NOUVELLE ANNEXE 19 — GESTION DE LA SÉCURITÉ

3.4.1 La nécessité d'élaborer une Annexe unique consacrée aux responsabilités et aux processus de gestion de la sécurité a fait l'objet d'une recommandation lors de la Conférence des directeurs généraux de l'aviation civile sur une stratégie globale pour la sécurité de l'aviation, tenue à Montréal du 20 au 22 mars 2006 (DGCA/06) et de la Conférence de haut niveau sur la sécurité, tenue également à Montréal, du 29 mars au 1^{er} avril 2010 (HLSC/2010).

3.4.2 Selon les instructions de ces conférences, la Commission est convenue d'établir le Groupe d'experts en gestion de la sécurité (SMP), chargé d'élaborer des recommandations pour l'élaboration d'une nouvelle Annexe consacrée aux responsabilités et aux processus de gestion de la sécurité.

3.4.3 En février 2012, le groupe d'experts SMP a recommandé le transfert des dispositions relatives à la gestion de la sécurité des Annexes 1 ; 6, Parties 1, 2 et 3 ; 8 ; 11 ; 13 et 14, Volume I (voir Tableaux 3-1 et 3-2) dans la nouvelle Annexe 19. La plupart de ces spécifications ont été modifiées pour plus de cohérence et de clarté, tout en maintenant l'exigence initiale pour laquelle elles ont été adoptées.

3.4.4 Les dispositions de l'Annexe 19, proposées par le SMP, sont destinées à harmoniser la mise en œuvre des pratiques de gestion de la sécurité pour les États et les organismes qui interviennent dans les activités de l'aviation. L'Annexe 19 comprend donc des spécifications relatives à la gestion de la sécurité à l'intention des États, des fournisseurs de produits et de services, ainsi que des exploitants d'avions utilisés dans l'aviation générale internationale. Certaines spécifications relatives à la gestion de la sécurité spécifiques à certains secteurs demeurent dans l'Annexe applicable au domaine d'activité de chacun des prestataires de services (p. ex. les spécifications relatives aux programmes d'analyse de données de vol pour exploitants aériens sont maintenues dans l'Annexe 6, Partie I).

3.4.5 Une fois adoptée, l'Annexe 19 aura un impact sur plusieurs Annexes de l'OACI à la Convention relative à l'aviation civile internationale. C'est pourquoi des amendements consécutifs des Annexes 1, 6, 8, 11, 13 et 14, découlant de l'adoption de l'Annexe 19, seront introduits simultanément afin d'éviter qu'il y ait des spécifications en double.

3.4.6 La date d'application de l'Annexe 19 est indépendante des dates d'application des dispositions existantes relatives à la gestion de la sécurité. La date d'application de l'Annexe 19 n'affecte donc pas l'applicabilité existante des SARP relatives à la gestion de la sécurité que contiennent d'autres Annexes.

Chapitre 4

PROGRAMME NATIONAL DE SÉCURITÉ (PNS)

4.1 INTRODUCTION

4.1.1 Le présent chapitre présente les objectifs, le cadre et la démarche de mise en œuvre d'un Programme national de sécurité (PNS). Il fait également l'analyse de l'importance d'établir des processus pour le maintien et l'évaluation de l'efficacité du PNS.

4.1.2 Un PNS est un système de gestion visant la réglementation et l'administration de la sécurité par l'État. La mise en œuvre d'un PNS dépend de l'ampleur et de la complexité du système d'aviation civile d'un État et nécessite la coordination entre les autorités multiples chargées des fonctions d'aviation de cet État. Le PNS a pour objet :

- a) d'assurer que l'État a mis en place un cadre réglementaire minimal ;
- b) de réaliser l'harmonisation entre les organes de réglementation et les organes d'administration de l'État dans leurs rôles respectifs de gestion des risques de sécurité ;
- c) de faciliter la surveillance et l'évaluation des performances globales de sécurité de l'industrie de l'aviation de l'État ;
- d) de coordonner et de renforcer de façon continue les fonctions de gestion de la sécurité de l'État ;
- e) d'appuyer la mise en œuvre et l'interaction efficaces avec les SGS des fournisseurs de services.

4.1.3 Les principes de gestion de la sécurité constituent une base pour l'établissement parallèle du PNS par l'État et des SGS par ses fournisseurs de services. En mettant en place le cadre législatif de la sécurité, l'État promulgue des exigences en matière de SGS, forçant les fournisseurs de services à mettre en œuvre leurs capacités de gestion de la sécurité afin de détecter effectivement les lacunes systémiques de sécurité et de résoudre les problèmes de sécurité.

4.1.4 Les SGS des fournisseurs de services doivent faire l'objet d'une surveillance réglementaire efficace. Par ailleurs, un SGS est essentiellement un système axé sur les performances qui dépend de l'échange approprié d'informations de sécurité avec des acteurs internes et externes. Par ses fonctions PNS, l'État s'acquitte de ses fonctions de supervision et facilite les activités de regroupement des données appropriées et de partage d'informations.

4.2 CADRE DU PNS

4.2.1 Quatre composants constituent la base d'un PNS. Chacun de ces composants se compose d'éléments qui comprennent les processus ou les activités entrepris par l'État pour la gestion de la sécurité. Ces 11 éléments, qui combinent à la fois des méthodes prescriptives et des démarches fondées sur les performances, soutiennent la mise en œuvre de SGS par les fournisseurs de services. Les quatre composants et les 11 éléments constituant le cadre d'un PNS sont énumérés ci-après :

1. Politiques et objectifs de sécurité de l'État
 - 1.1 Cadre législatif national de la sécurité
 - 1.2 Responsabilités et imputabilités de sécurité de l'État
 - 1.3 Enquête sur les accidents et les incidents
 - 1.4 Politiques d'application
2. Gestion des risques de sécurité de l'État
 - 2.1 Exigences de sécurité pour les SGS des fournisseurs de services
 - 2.2 Accord sur les performances de sécurité des fournisseurs de services
3. Assurance de sécurité de l'État
 - 3.1 Supervision de la sécurité
 - 3.2 Collecte, analyse et échange des données de sécurité
 - 3.3 Ciblage fondé sur les données de sécurité pour la surveillance des domaines présentant les inquiétudes ou les besoins les plus graves
4. Promotion de la sécurité par l'État
 - 4.1 Formation, communication et diffusion à l'interne des informations de sécurité
 - 4.2 Formation, communication et diffusion à l'externe des informations de sécurité.

4.2.2 Les sections qui suivent donnent une brève description des composants et des éléments du cadre d'un PNS.

Composant 1 du PNS. Politiques et objectifs de sécurité de l'État

4.2.3 Le composant « Politiques et objectifs de sécurité de l'État » définit la manière dont l'État gèrera la sécurité dans son système d'aviation. Il comprend la détermination des responsabilités et des imputabilités des différents organismes d'État liés au PNS, ainsi que les objectifs généraux de sécurité visés par le PNS.

4.2.4 Les politiques et les objectifs de sécurité de l'État fournissent aux administrateurs et au personnel des politiques claires, des directives, des procédures, des mesures de contrôle de gestion, des documents et des processus de mesures correctrices qui maintiennent sur la bonne voie les activités de gestion de la sécurité menées par les autorités d'aviation civile et les autres organismes de l'État. Ceci permet à l'État d'assurer le leadership dans le domaine de la sécurité dans un système de transport aérien complexe et en évolution constante. L'Appendice 1 au présent chapitre contient des orientations sur l'élaboration d'une déclaration de politique de la sécurité de l'État.

Élément 1.1 du PNS Cadre législatif national de la sécurité

L'État a promulgué un cadre législatif national de la sécurité et des règlements spécifiques, en conformité avec les normes nationales et internationales, qui définissent la façon dont il assurera la gestion de la sécurité dans l'État. Ceci inclut la participation des organismes nationaux de l'aviation dans des activités particulières liées à la gestion de la sécurité au sein de l'État, ainsi que la détermination des rôles de ces organismes, de leurs responsabilités et de leurs rapports respectifs. Le cadre législatif de la sécurité et les règlements particuliers font l'objet d'un examen périodique afin d'en assurer la pertinence et le bien-fondé pour l'État.

4.2.5 Un cadre législatif national de la sécurité doit être établi et modifié s'il y a lieu. Ce cadre couvrira tous les secteurs de l'aviation et les fonctions administratives applicables à l'État et sera conforme aux normes internationales. Une telle législation définit clairement les rôles et les responsabilités de tout organisme d'État assurant des fonctions réglementaires ou administratives dans le domaine de l'aviation. Il se peut que certains cadres législatifs puissent comprendre des lois distinctes qui auraient été élaborées séparément pour différents ministères. Ainsi, par exemple, le cadre législatif portant sur la responsabilité de l'État de l'administration et de l'exploitation directe des aéroports et des services ATS aurait pu être établi séparément au fil des ans. Une telle législation se serait concentrée sur ces deux secteurs, mettant l'accent sur les aspects opérationnels et techniques de l'apport de ces services. Un cadre législatif comportant un tel angle opérationnel risque de faire obstacle à une coordination adéquate des activités de gestion de la sécurité de tous les organes compétents de l'État.

4.2.6 Un mécanisme d'examen périodique du cadre législatif aéronautique complet assurera une amélioration continue et la corrélation entre la législation et les besoins de règlements opérationnels. Bien que l'examen des exigences opérationnelles particulières relève de la compétence des organes de réglementation respectifs, l'intégration et la cohésion nécessaires des lois de plus haut niveau doivent être assurées par une plate-forme de coordination à l'échelle nationale, surtout si plusieurs organismes et ministères sont impliqués.

Élément 1.2 du PNS Responsabilités et imputabilités de sécurité de l'État

L'État a déterminé, défini et documenté les exigences, les responsabilités et les imputabilités concernant l'établissement et le maintien à jour du PNS. Elles comprennent les tâches de planification, d'organisation, d'établissement, de tenue à jour, de contrôle et d'amélioration constante du PNS de façon à répondre aux objectifs de sécurité de l'État. Elles incluent aussi une déclaration claire sur la mise à disponibilité des ressources nécessaires à la mise en œuvre du PNS.

4.2.7 La responsabilité initiale de l'État dans la mise en œuvre du PNS est de déterminer l'administrateur responsable du PNS ainsi que l'organisme qui sera chargé de l'administration et de la coordination de la mise en œuvre et du fonctionnement du PNS. Dans le présent document, l'entité en question est également appelée organisation signet du PNS.

4.2.8 Dans le cas des États où plusieurs organes de réglementation et d'administration sont impliqués, il pourrait être nécessaire d'identifier en outre un comité national compétent où ces organes seraient représentés, pour servir de plate-forme nationale permanente de coordination.

4.2.9 L'administrateur responsable et l'organisation signet désignés commenceront le processus de mise en œuvre du PNS en mettant sur pied une équipe de mise en œuvre du PNS. Cette équipe sera chargée de travailler en coopération avec l'administrateur responsable et les divers organismes pour entamer le processus de planification et d'exécution du PNS.

4.2.10 La mise en œuvre du PNS et son fonctionnement continu devront être définis et documentés. Le système de documentation du PNS devrait inclure un document de haut niveau définissant/décrivant le PNS, ainsi que d'autres dossiers, formulaires et PON portant sur la mise en œuvre et le fonctionnement du PNS.

4.2.11 Parallèlement à la définition des responsabilités et des imputabilités en matière de gestion de la sécurité, il convient de procéder à l'élaboration coordonnée d'une politique (déclaration) nationale de la sécurité, applicable dans le cadre réglementaire et administratif de l'État. De même, les objectifs généraux de sécurité de l'État font partie des déclarations générales de mission de tous les organismes nationaux compétents. Les objectifs de sécurité de haut niveau peuvent alors être appuyés par les indicateurs de sécurité appropriés afin d'en faciliter l'évaluation ou la mesure selon qu'il convient.

Élément 1.3 du PNS Enquête sur les accidents et incidents

L'État a établi un processus indépendant d'enquête sur les accidents et incidents, dont le seul objectif est de prévenir les accidents et les incidents et non pas d'attribuer les blâmes ou les responsabilités. Ces enquêtes appuient la gestion de la sécurité de l'État. Dans le fonctionnement du PNS, l'État maintient l'indépendance de l'organisation des enquêtes sur les accidents et incidents par rapport aux autres organismes aéronautiques de l'État.

4.2.12 Du point de vue du PNS, la fonction d'enquête sur les accidents et incidents est axée sur son administration à l'échelle nationale. Une organisation ou une entité d'enquête fonctionne indépendamment de tout autre organisme, et en particulier de l'autorité de l'aviation civile de l'État, dont les intérêts pourraient entrer en conflit avec les tâches confiées à l'autorité chargée de l'enquête. La raison fondamentale pour laquelle cette fonction est indépendante de celles des autres organismes est que la cause d'un accident peut être due à des facteurs de réglementation ou liée au PNS. En outre, une telle indépendance permet de renforcer la viabilité de l'organisation d'enquête et d'éviter les conflits d'intérêts réels ou perçus.

4.2.13 Certains États peuvent ne pas disposer des ressources requises pour s'acquitter de leurs responsabilités en matière d'enquête. Dans ces cas, l'adhésion à un organisme régional d'enquête sur les accidents et incidents (RAIO) serait un moyen viable de réaliser l'intention d'un processus d'enquête indépendant. À cette fin, nous appelons l'attention du lecteur sur le *Manuel sur les organismes régionaux d'enquête sur les accidents et incidents* de l'OACI (Doc 9946).

Élément 1.4 du PNS Politique d'exécution

L'État a promulgué une politique d'exécution qui établit les conditions et les circonstances dans lesquelles les fournisseurs de services sont autorisés à traiter et à résoudre à l'interne des événements comportant certains écarts à la sécurité, dans le contexte du système de gestion de la sécurité (SGS) de ces fournisseurs de services, à la satisfaction de l'autorité nationale compétente. La politique d'exécution établit en outre les conditions et les circonstances dans lesquelles les écarts à la sécurité sont traités selon les procédures d'exécution établies.

4.2.14 À l'instar de toute autre législation nationale, on peut s'attendre à ce que le cadre législatif de l'aviation puisse inclure une disposition de base pour des mesures d'exécution. Une telle disposition se limiterait probablement à couvrir uniquement la portée des sanctions en cas d'infraction. Dans un environnement PNS-SGS, l'intention est que les politiques et les procédures d'exécution, que ce soit au niveau du fournisseur de services ou au niveau de l'État (AAC), soient renforcées pour incorporer des dispositions régissant la nature et la portée des mesures exécutoires ou disciplinaires, selon les conditions et les circonstances entourant une infraction ou un acte de non-conformité. L'objet

d'un tel renforcement est d'assurer qu'une distinction nécessaire soit établie entre une infraction délibérée/flagrante et une erreur/faute non intentionnelle.

4.2.15 Pour permettre un tel renforcement, l'État doit manifester son intention par des politiques et des procédures d'exécution. Il doit également énoncer formellement à ses fournisseurs de services la nécessité de procédures disciplinaires incorporant un renforcement équivalent. Cela signifie que les fournisseurs de services sont censés avoir mis en place un processus acceptable de gestion de leurs propres écarts de sécurité/qualité opérationnelle au moyen de politiques et de procédures disciplinaires internes. L'État indiquerait que des interventions réglementaires seraient exécutées dans certaines conditions et circonstances, au cours desquelles l'État (AAC) se chargera du processus d'enquête pour une infraction ou un état de non-conformité particulier.

Composant 2 du PNS. Gestion de risques de sécurité de l'État

4.2.16 Le composant de gestion de risques de sécurité de l'État comprend l'établissement des exigences en matière de SGS pour assurer que chaque fournisseur de services applique les processus d'identification des dangers et les mesures de gestion des risques nécessaires. Ces exigences incluent notamment un mécanisme d'accord avec les différents fournisseurs de services sur les niveaux de performance acceptables en matière de sécurité à assurer grâce à leurs SGS.

4.2.17 En plus d'assurer que les fournisseurs de services se chargent effectivement de l'identification des dangers et de la gestion des risques prévues dans leurs SGS, l'État peut en outre appliquer les principes de gestion des risques de sécurité à ses propres activités de réglementation et de PNS. L'élaboration de règles, la sélection d'indicateurs de sécurité pour le PNS, l'établissement de cibles et de niveaux d'alertes correspondants et la priorisation des programmes de surveillance, sont autant de processus qui pourraient être renforcés par une démarche axée sur les risques et fondée sur les données.

4.2.18 Les risques graves révélés par l'analyse des données de sécurité internes d'un fournisseur de services et de ses performances en matière de sécurité, peuvent nécessiter une coordination ou un accord avec l'autorité de réglementation de l'aviation de l'État, qui tiendrait compte des mesures d'atténuation appropriées, surtout si ces risques sont susceptibles d'avoir des incidences sur les autres fournisseurs de services ou sur d'autres parties intéressées.

Élément 2.1 du PNS Exigences en matière de sécurité pour les SGS des fournisseurs de services

L'État a établi les mesures de contrôle qui déterminent la façon dont les fournisseurs de services identifieront les dangers et géreront les risques de sécurité. Ces mesures comprennent des spécifications, des règlements opérationnels particuliers et des politiques de mise en œuvre pour les SGS des fournisseurs de services. Ces spécifications, ces règlements et ces politiques sont revus périodiquement pour en assurer la pertinence et le bien-fondé pour les fournisseurs de services.

4.2.19 L'État établit les exigences en matière de sécurité pour le SGS d'un fournisseur de services en promulguant des règlements qui définissent les composants et les éléments requis du cadre du SGS. Au sein de ce cadre, l'exécution effective du composant de gestion des risques de sécurité (SRM) permettra d'assurer que les fournisseurs de services identifient les dangers et gèrent les risques connexes. Les procédures détaillées de chaque fournisseur de services pour l'identification des dangers et la gestion des risques dépendront de la complexité de

chaque organisation et seront décrites en conséquence dans les documents sur le SGS. Pour des entités non réglementées telles que les sous-traitants, il pourrait être demandé d'une organisation au SGS approuvé qu'elle exige (contractuellement) de ses sous-traitants des processus d'identification des dangers et de gestion des risques, le cas échéant. Dans le cas d'un sous-traitant disposant d'un SGS accepté, il faudra résoudre la question de l'intégration nécessaire.

4.2.20 Les exigences réglementaires de l'État pour les SGS et les éléments indicatifs connexes doivent être révisées périodiquement, en tenant compte des rétroactions de l'industrie, ainsi que de la situation en vigueur et de l'applicabilité des SARP et des éléments d'orientation de l'OACI sur les SGS.

**Élément 2.2 du PNS Accord sur les performances de sécurité
des fournisseurs de services**

L'État est convenu avec les différents fournisseurs de services sur les performances de sécurité de leurs SGS. Les performances de sécurité convenues du SGS d'un fournisseur de services sont revues périodiquement pour en assurer la pertinence et le bien-fondé pour le fournisseur de services.

4.2.21 Dans le cadre du processus d'acceptation du SGS, les indicateurs de performance de sécurité (SPI) proposés du fournisseur de services et les cibles et alertes connexes sont examinés et convenus par l'organisme de réglementation compétent de l'État. Il est aussi possible pour l'État d'accepter un plan de mise en œuvre du SGS d'un fournisseur de services en vue de l'approbation ultérieure de ses SPI, dans le cadre du processus de mise en œuvre de son SGS. Dans tous les cas, l'acceptation complète d'un SGS signifie que l'organisme de réglementation convient que les SPI proposés sont appropriés et pertinents pour les activités aéronautiques du fournisseur de services intéressé.

4.2.22 Il est possible que ce processus d'acceptation des performances de sécurité puisse inclure par la suite l'exécution d'évaluations de sécurité particulières ou de mesures d'atténuation de risques par le fournisseur de services. Cette étape peut résulter de risques particuliers révélés par des sources telles que le fournisseur de services, l'industrie, l'État ou des données de sécurité générales.

4.2.23 Les SPI et les cibles et niveaux d'alerte connexes de chaque fournisseur de services devraient faire l'objet d'examens périodiques. Ces examens tiendraient compte des performances et de l'efficacité de chaque SPI et de ses cibles et alertes connexes. Toute modification requise des SPI, des cibles ou niveaux d'alerte précédemment approuvés, devrait être justifiée par des données de sécurité appropriées et étayée par des pièces justificatives.

Composant 3 du PNS. Assurance de sécurité par l'État

4.2.24 L'assurance de sécurité par l'État est accomplie par des activités de supervision et de surveillance des fournisseurs de services, ainsi que par l'examen interne par l'État de ses processus réglementaires et administratifs. Le rôle important de la collecte des données de sécurité, de leur analyse et de leur diffusion est également couvert. Les programmes de surveillance de l'État devraient être fondés sur les données, afin de concentrer et de prioriser les ressources en fonction des domaines présentant les risques ou les problèmes de sécurité les plus graves.

Élément 3.1 du PNS Supervision de la sécurité

L'État a mis en place des mécanismes pour assurer une surveillance efficace des huit éléments critiques de la fonction de supervision de la sécurité. Il a également établi des mécanismes pour assurer l'identification des dangers et la gestion des risques de sécurité par les fournisseurs de services en appliquant des mesures de réglementation établies (spécifications, règlements opérationnels spécifiques et politiques de mise en œuvre). Ces mécanismes incluent des inspections, des audits et des enquêtes pour assurer que des mesures de réglementation des risques de sécurité sont intégrées comme il faut dans les SGS des fournisseurs de services, qu'elles sont appliquées conformément à leur fonction prévue et que les mesures de réglementation ont l'effet visé sur les risques de sécurité.

4.2.25 La mise en œuvre des SARP de l'OACI constitue la base de la stratégie de sécurité aérienne d'un État. L'élément 3.1 du PNS couvre les méthodes suivies par l'État pour surveiller efficacement l'établissement et la mise en œuvre de son système de supervision de la sécurité. On trouvera les détails sur les éléments critiques d'un système national de supervision de la sécurité dans le Doc 9734, Partie A.

4.2.26 Le système de supervision de la sécurité de l'État inclut des obligations liées à l'approbation initiale et à la surveillance continue de ses fournisseurs de services aéronautiques pour assurer qu'ils sont conformes aux règlements nationales établies en conformité avec les SARP de l'OACI.

Note.— Le processus d'approbation initiale comprend l'autorisation, la certification ou la désignation par l'État des fournisseurs de services appropriés.

4.2.27 L'autorisation initiale, la certification ou la désignation par l'État d'un fournisseur de services incluent l'acceptation du plan de mise en œuvre du SGS de l'organisation. Certains éléments du plan de mise en œuvre du SGS du fournisseur de services auront été mis en place au moment de l'approbation initiale de l'organisation, alors que d'autres éléments ne seront mis en œuvre qu'après la démarche par étapes décrite au Chapitre 5.

4.2.28 L'État s'acquitte de ses obligations de surveillance au moyens d'audits et d'inspections pour assurer que les fournisseurs de services maintiennent un niveau adéquat de conformité aux règlements et qu'ils exécutent leurs activités aéronautiques respectives en respectant la sécurité. Les obligations de surveillance de l'État comprennent en outre l'acceptation d'un SGS mis en œuvre par chacun de ses fournisseurs de services existants, ainsi qu'une évaluation périodique des performances des SGS.

4.2.29 Les activités de surveillance et d'examen de l'État, incluant toutes mesures connexes recommandées, sont coordonnées aux fins d'évaluation ou de résolution au niveau de la plate-forme nationale de coordination du PNS, s'il y a lieu.

Élément 3.2 du PNS Collecte, analyse et échange de données de sécurité

L'État a établi des mécanismes pour assurer la capture et l'entreposage de données sur les dangers et les risques de sécurité sur une base individuelle aussi bien que globale au niveau de l'État. L'État a aussi établi des mécanismes pour tirer des informations des données entreposées, et pour échanger activement des informations de sécurité avec les fournisseurs de services et/ou avec d'autres États le cas échéant.

4.2.30 L'État a établi un système de collecte et de traitement de données de sécurité (SDCPS) pour assurer la capture, l'entreposage et le regroupement des données sur les accidents, les incidents et les dangers qui figurent dans les rapports obligatoires et volontaires de l'État. Un tel système devrait être fondé sur l'exigence imposée par l'État aux fournisseurs de services de lui signaler les accidents, les incidents graves et tous autres incidents considérés par l'État comme devant être signalés. Il convient d'établir une distinction appropriée entre, d'une part, les rapports d'accident et d'incident et d'autre part, les rapports sur les dangers. De même, il convient de distinguer entre les systèmes de comptes rendus obligatoires (réglementaires) et les systèmes de comptes rendus volontaires, notamment les exigences appropriées de confidentialité pour les systèmes volontaires. L'Appendice 2 contient des orientations sur un système national de compte rendu volontaire, tandis que l'Appendice 3 donne un exemple de procédure de compte rendu obligatoire d'un État.

4.2.31 La capture de données sur les accidents et les incidents à déclaration obligatoire devrait inclure les rapports d'enquête pertinents. Les rapports volontaires soumis peuvent nécessiter une certaine forme de suivi ou d'évaluation pour en vérifier la validité. Les rapports de danger vérifiés devront peut-être faire l'objet de suivi sous forme d'une évaluation de risque et d'un processus d'atténuation au niveau des fournisseurs de services ou de l'AAC, selon le cas. Les divers types de données de sécurité peuvent être regroupées dans un SDCPS centralisé ou recueillies et archivées dans des modules intégrés d'un réseau SDCPS distribué, selon le cas.

4.2.32 L'État a également établi des procédures pour extraire et traiter des informations des données groupées entreposées et pour partager activement les informations de sécurité avec des fournisseurs de services et/ou avec d'autres États, s'il y a lieu. La disponibilité de ces sources de données de sécurité permet à l'État de créer des indicateurs de sécurité pour le PNS, tels que les taux d'accident et d'incident. Les indicateurs de sécurité établis et leurs cibles et niveaux d'alerte respectifs serviront de mécanisme de mesure et de surveillance de la sécurité (ALoSP). De plus amples détails sur l'établissement d'indicateurs de sécurité figurent dans les paragraphes 4.3.5.1 à 4.3.5.12 et dans l'Appendice 4 au présent chapitre.

4.2.33 Afin d'assurer la disponibilité continue des données de sécurité, notamment avec les systèmes de compte rendu volontaires, le SDCPS devrait fournir des informations appropriées pour la protection de la sécurité. L'Appendice 5 contient des éléments d'orientation sur ces informations.

4.2.34 Les États disposant de multiples autorités chargées de la réglementation de la sécurité devraient assurer la réglementation de la sécurité, une coordination appropriée, l'intégration et l'accessibilité de leurs bases de données de sécurité liées au PNS. La directive s'applique également aux États où le processus d'enquête sur les accidents est confié à un organisme indépendant de l'AAC. Les mêmes dispositions peuvent être envisagées pour les États dont certaines fonctions de gestion de la sécurité (incluant le traitement de données liées au PNS) sont assurées en leur nom par une RSOO ou une RAIO.

4.2.35 Le SDCPS de l'État inclura des procédures de soumission de rapports d'accident et d'incident à l'OACI, qui faciliteront la collecte et le partage des informations de sécurité à l'échelle mondiale. L'Appendice 6 au présent chapitre contient des directives sur la notification et le compte rendu d'accident et d'incident, conformément aux dispositions de l'Annexe 13 de l'OACI.

Élément 3.3 du PNS Ciblage axé sur les données de sécurité pour la supervision de domaines présentant des problèmes ou des besoins plus importants

L'État a établi des procédures de priorisation des inspections, des audits et des enquêtes pour les domaines présentant des problèmes ou des besoins plus importants, déterminés par l'analyse des données sur les dangers, leurs conséquences sur les opérations et les risques évalués de sécurité.

4.2.36 Des programmes réguliers de supervision, de surveillance ou d'inspection tendent à être appliqués systématiquement et invariablement à tous les fournisseurs de services, sans prévoir de mécanisme de modulation de la fréquence ou de la portée des activités de surveillance en fonction des circonstances. Un environnement de gestion de la sécurité permettrait une évaluation plus dynamique des performances de sécurité. Dans le cadre du PNS, les programmes de supervision et de surveillance réglementaires devraient inclure un mécanisme permettant d'adapter la portée ou la fréquence de la surveillance aux performances concrètes. Une telle démarche de priorisation fondée sur les risques facilitera la répartition des ressources aux domaines présentant les plus grands risques, problèmes ou besoins. Les données à utiliser pour une telle modulation de la surveillance peuvent inclure des indicateurs de performance liés à des secteurs d'activités aéronautiques particuliers, ainsi que les résultats tirés de rapports de surveillance ou d'audits antérieurs de divers fournisseurs de services. Il convient d'établir à cette fin des critères de quantification des résultats (p. ex. un taux de conformité effective) pour chaque audit réalisé.

4.2.37 Une méthode plus complète de surveillance fondée sur les risques pourrait inclure des éléments de données sur les risques de sécurité qui seraient extérieurs au programme de surveillance. Ces éléments supplémentaires de modulation de la fréquence ou de la portée de la surveillance peuvent provenir, par exemple, d'un programme d'évaluation de l'ORP (voir le Chapitre 2, Appendice 1, pour les détails sur le concept d'évaluation de l'ORP). D'autres éléments/problèmes peuvent aussi provenir du SDCPS de l'État ou des indicateurs de sécurité. Il convient d'avoir les interactions appropriées avec les fournisseurs de services avant de procéder à la modification d'activités de surveillance quelconques. La Figure 4-1 présente une illustration du concept amélioré de supervision/ surveillance fondée sur les données de sécurité et les risques.

Composant 4 du PNS. Promotion de la sécurité par l'État

4.2.38 La promotion de la sécurité comprend l'établissement par l'État de processus internes aussi bien qu'externes pour assurer ou faciliter la formation à la sécurité, les communications et la diffusion des informations de sécurité.

Élément 4.1 du PNS Formation, communication et diffusion à l'interne des informations de sécurité

L'État assure la formation et encourage la sensibilisation aux risques de sécurité ainsi que les communications bilatérales d'informations liées à la sécurité, afin d'appuyer la création, au sein des organismes aéronautiques de l'État, d'une culture organisationnelle qui soutient un PNS efficace et efficient.

4.2.39 Les organismes nationaux de réglementation responsables des différents secteurs de l'aviation, ainsi que d'autres entités administratives indépendantes telles que les services d'enquête sur les accidents, devraient adopter une démarche intégrée dans l'exécution de leurs rôles respectifs. Il importe donc de veiller à ce qu'ils disposent entre eux d'une voie de communication spéciale pour la sécurité, et en particulier, d'une organisation signet pour le PNS. La documentation relative au PNS et les politiques nationales de sécurité et d'exécution connexes sont essentielles pour réaliser l'intégration de la formation, de la communication et de la diffusion des informations pertinentes. Toutes autres stratégies opérationnelles ultérieures relatives au PNS, notamment les exigences harmonisées des SGS et la supervision des fournisseurs de services respectifs, devraient être partagées, communiquées et coordonnées entre les organisations. Cela permettra d'éviter de créer des exigences contradictoires pour les SGS ou des critères de supervision/d'acceptation les différents secteurs de l'aviation.

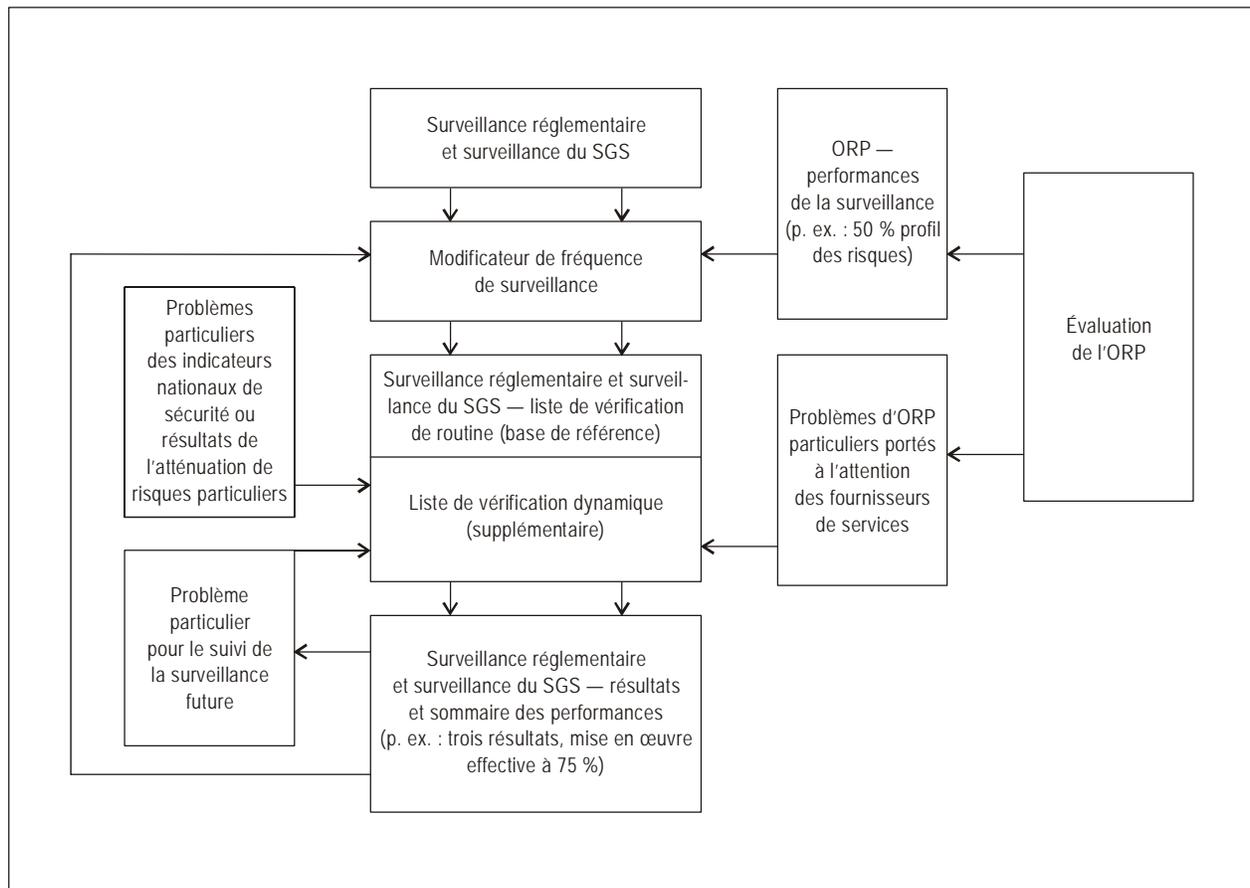


Figure 4-1. Concept de surveillance fondé sur les données de sécurité et les risques

4.2.40 Il convient de coordonner entre les diverses organisations nationales les programmes internes de formation à la sécurité destinés au personnel affecté aux fonctions liées au PNS. La formation au PNS et au SGS devrait être accordée en priorité au personnel participant à la mise en œuvre ou à la supervision de ces programmes, en particulier les inspecteurs d'opérations ou les inspecteurs sur le terrain qui participeront à la détermination des critères d'acceptation des SGS ou à d'autres questions de performance de la sécurité. La portée des textes de formation/familiarisation aux PNS et SGS évoluera pour tenir compte des processus réels du PNS de l'État à mesure qu'ils sont pleinement appliqués. La formation aux PNS et SGS peut se limiter initialement aux éléments génériques du cadre PNS/SGS et aux éléments d'orientations tels que ceux qui figurent dans les cours de formation aux PNS/SGS de l'OACI.

Élément 4.2 du PNS Formation, communication et diffusion à l'externe des informations de sécurité

L'État assure la formation et encourage la sensibilisation aux risques de sécurité ainsi que les communications bilatérales d'informations liées à la sécurité, afin d'appuyer la création, parmi les fournisseurs de services, d'une culture organisationnelle qui soutient des SGS efficaces et efficients.

4.2.41 L'État devrait disposer d'une plate-forme ou d'un support approprié de communication pour faciliter la mise en œuvre des SGS. Il peut s'agir d'un support intégré destiné aux fournisseurs de services dans tous les secteurs de l'aviation, ou d'un canal de l'organisme de réglementation compétent réservé aux fournisseurs de services placés sous sa juridiction. Le contenu essentiel de ces communications extérieures sur les SGS et la sécurité concerne les spécifications et les éléments d'orientation sur les SGS. La documentation sur le PNS et ses politiques nationales connexes sur la sécurité et l'exécution devraient également être mises à la disposition des fournisseurs de services, selon qu'il convient. Ces voies de communication externe peuvent aussi être renforcées afin d'inclure d'autres questions liées à la sécurité, le cas échéant. Il faudrait de préférence prévoir des communications bilatérales pour permettre la rétroaction de l'industrie.

4.2.42 L'État devrait en outre faciliter la formation ou la familiarisation de ses fournisseurs de services aux SGS, dans la mesure du possible et selon qu'il convient.

4.3 PLANIFICATION DE LA MISE EN ŒUVRE DU PNS

4.3.1 Généralités

Le PNS d'un État doit être adapté à la taille et à la complexité de son système d'aviation, ce qui pourrait appeler une coordination entre les multiples organisations de réglementation de l'aviation responsables de leurs secteurs respectifs. La mise en œuvre d'un PNS ne devrait pas modifier les rôles respectifs des organisations aéronautiques de l'État, ni l'interaction normale entre elles. Au contraire, le PNS renforce les fonctions et capacités collectives de réglementation et d'administration qu'elles exercent au nom de l'État. D'ailleurs la plupart des États disposent déjà de processus qui répondent aux attentes de certains éléments du PNS. Il s'agit de les regrouper et de les renforcer avec d'autres éléments fondés sur les performances et les risques, de manière à aboutir à une gestion intégrée du cadre de la sécurité. Ce cadre du PNS facilitera également la mise en œuvre et la supervision efficaces des SGS par l'industrie. La présente section soulignera certaines considérations importantes de la mise en œuvre du PNS.

4.3.2 Description du système de réglementation

L'examen du système de réglementation fait partie du processus de planification de la mise en œuvre du PNS. Un tel examen devrait inclure une description des éléments suivants :

- a) la structure du cadre existant de réglementation de l'aviation, allant du niveau ministériel jusqu'à celui des diverses organisations de réglementation ou d'administration ;
- b) les rôles et les responsabilités de gestion de la sécurité des diverses organisations de réglementation ;
- c) la plate-forme ou le mécanisme aux fins de la coordination du PNS entre les organisations ;
- d) un mécanisme interne d'examen de la sécurité/qualité au niveau de l'État et au sein de chaque organisation.

La documentation du PNS devrait inclure la structure ou l'organigramme des organisations de réglementation et d'administration de l'État.

4.3.3 Analyse des carences

Avant d'établir un plan de mise en œuvre du PNS, il convient de procéder à une analyse des carences des structures et des procédures existantes de l'État en comparaison avec le cadre PNS de l'OACI, afin de déterminer l'existence et la maturité des éléments respectifs du PNS. À l'issue de cette analyse, les éléments ou procédures identifiés comme nécessitant des corrections constitueront la base du plan de mise en œuvre du PNS. L'Appendice 7 au présent chapitre contient d'autres éléments indicatifs sur la procédure d'analyse des carences du PNS.

4.3.4 Plan de mise en œuvre du PNS

À l'instar de toute initiative importante de projet de mise en œuvre, l'exécution du PNS comprend de nombreuses tâches et sous-tâches à réaliser suivant un calendrier établi. Le nombre de tâches et leur portée respective dépendent de la maturité du système de supervision de la sécurité en place. L'objectif du processus de mise en œuvre est d'assurer une amélioration effective des processus existants de gestion, d'administration et de supervision de la sécurité. Les tâches/sous-tâches appropriées sont priorisées et documentées sous une forme appropriée aux fins d'exécution progressive. Le plan de mise en œuvre du PNS, ainsi qu'un document (de présentation) de haut niveau du PNS, constituent le fondement à partir duquel un État entreprendra le renforcement progressif de ses processus de gestion, d'administration et de supervision de la sécurité. Ces deux documents clés devraient être rendus facilement accessibles à tout le personnel compétent au sein de l'organisation, afin de faciliter la sensibilisation au PNS et l'avancement des travaux de mise en œuvre. La section 4.4 et l'Appendice 7 au présent chapitre contiennent d'autres éléments d'orientation sur le plan de mise en œuvre du PNS.

4.3.5 Indicateurs de sécurité

Niveau acceptable de performance de sécurité

4.3.5.1 Le concept de niveau acceptable de performance de sécurité (ALoSP) vient s'ajouter à la démarche traditionnelle de supervision de la sécurité axée essentiellement sur la conformité réglementaire prescriptive, pour établir une approche fondée sur les performances qui définit des niveaux effectifs de performance de sécurité dans le cadre prescrit du PNS. Aux fins du présent manuel, l'ALoSP est le niveau acceptable de performance de sécurité d'un État, tel qu'il est défini par les indicateurs de sécurité du PNS et les cibles et niveaux d'alertes connexes. Un ALoSP national devrait être pertinent aux politiques et objectifs de sécurité de l'État.

4.3.5.2 Les critères régissant l'ALoSP national peut varier selon le contexte particulier du système d'aviation de chaque État et la maturité de son système de supervision de la sécurité. Le but essentiel est de réaliser la conformité aux dispositions de l'OACI et de réduire le nombre d'événements à conséquences graves lorsque les problèmes sont évidents. Le but final aboutira à l'engagement de l'État à améliorer constamment les performances de sécurité. Une fois établi, l'ALoSP d'un PNS donné est la manifestation de ce que l'État considère approprié dans le contexte de son propre système d'aviation. L'ALoSP d'un État exprime également les objectifs minimaux de sécurité acceptables à l'autorité de supervision que l'ensemble des fournisseurs de services placés sous son contrôle doivent réaliser.

4.3.5.3 Aux fins d'un PNS, l'ALoSP est identifié et établi par les indicateurs de sécurité globaux de l'État. Les indicateurs utilisés à cette fin incorporent des objectifs visés et des niveaux d'alerte, le cas échéant. L'ALoSP est donc le concept général, tandis que les niveaux d'alerte et de cibles (établissement des limites des performances) correspondants en sont les critères de référence effectifs. Le taux de réalisation des objectifs des indicateurs de sécurité est la mesure de performance de ces indicateurs. L'Appendice 4 contient des exemples illustratifs de l'élaboration d'indicateurs de sécurité de l'ALoSP.

4.3.5.4 Une procédure pleinement établie de surveillance et de mesure d'ALoSP permet les tâches ci-après, sur une base continue :

- a) identifier tous les secteurs critiques de la sécurité et les indicateurs de sécurité qui définissent le niveau de sécurité dans ces secteurs ;
- b) identifier les cibles qui définissent le niveau à maintenir ou les améliorations à apporter pour les indicateurs pertinents dans chacun de ces secteurs, afin de permettre l'amélioration constante de l'ensemble du système d'aviation ;
- c) identifier les alertes qui indiqueront un problème réel ou potentiel de performance dans un indicateur ou un secteur particulier de sécurité ;
- d) examiner les performances de sécurité du PNS pour déterminer s'il convient d'apporter des modifications ou des ajouts aux indicateurs, aux cibles ou aux alertes existants afin d'assurer une amélioration constante.

4.3.5.5 L'établissement d'indicateurs, de cibles et d'alertes de sécurité d'ALoSP pour un PNS ne remplace ni n'élimine la nécessité pour les États de se conformer à toutes les SARP applicables ni ne les libère de leurs obligations en vertu de la Convention relative à l'aviation civile internationale et de ses dispositions connexes.

Établissement d'alertes/de cibles

4.3.5.6 Les indicateurs de sécurité sont des outils tactiques de surveillance et de mesure des performances de sécurité de l'État. Durant l'élaboration initiale et la mise en œuvre d'un PNS, le niveau des performances de sécurité est représenté normalement par des indicateurs de sécurité liés à des résultats à conséquences élevées (tels que les taux d'accident et d'incident grave) et aux résultats d'évaluation de haut niveau (tels que la mise en œuvre effective des SARP de l'OACI). À mesure que le PNS prend de la maturité, le niveau des performances de sécurité peut être complété par des indicateurs représentant des résultats à plus faibles conséquences ou des occurrences d'écart. Les indicateurs de performances de sécurité sont généralement surveillés au moyen d'outils de mesure de tendances d'orientation avec des données quantitatives de base qui produisent des graphiques ou des tableaux incorporant des niveaux d'alerte/de cible communément utilisés dans les systèmes de contrôle technique, de qualité ou de fiabilité.

4.3.5.7 Les cibles définissent les objectifs de performances de sécurité à long terme du PNS. Exprimées en termes numériques, elles doivent être concrètes, mesurables, acceptables, fiables et pertinentes. Les cibles doivent en outre contenir des dates d'achèvement avec des étapes si elles doivent être réalisées par phases ou sur une longue période. Les cibles offrent une méthode mesurable d'assurer et de démontrer l'efficacité d'un PNS. L'établissement de cibles (quantum) devrait tenir compte de facteurs tels que le niveau applicable de risque de sécurité, les coûts et les avantages résultant des améliorations du système d'aviation, ainsi que des attentes concernant la sécurité de l'industrie de l'aviation de l'État. L'établissement de cibles d'améliorations désirées devrait être fondé sur ce qui est raisonnablement faisable pour le secteur aéronautique visé. Il doit tenir compte des performances historiques récentes d'un indicateur de sécurité particulier, si ces données historiques sont disponibles.

4.3.5.8 Un niveau d'alerte correspondant est déterminé pour chaque indicateur de performance de sécurité, établissant quantitativement le seuil de performance non acceptable (taux d'occurrence anormal) durant une période de surveillance spécifiée. L'utilisation de critères objectifs fondés sur des données pour l'établissement de niveaux d'alerte est essentielle pour faciliter l'exécution d'analyses cohérentes des tendances ou des références. La détermination d'un niveau d'alerte établit la démarcation entre les zones de performance acceptables des zones non acceptables d'un diagramme d'indicateurs de sécurité et constitue le facteur déclencheur principal (alerte/signal d'alarme) des mesures correctives liées à un indicateur de sécurité particulier. Tout dépassement du niveau d'alerte appellera une enquête de suivi pour en déterminer la cause et les mesures éventuelles de correction ou d'atténuation s'il y a lieu. Les mesures de

suivi nécessitent la coordination avec les fournisseurs de services intéressés afin de déterminer les causes fondamentales, les dangers et les risques connexes, selon le cas.

4.3.5.9 Comme pour les pratiques des critères de sécurité génériques, l'utilisation de l'écart-type de la population (STDEVP) constitue une méthode objective fondamentale d'établissement des critères d'alerte. Cette méthode consiste à déterminer la valeur de l'écart-type (SD) à partir des points de données historiques précédents d'un indicateur de sécurité donné. Cette valeur SD, additionnée à la valeur moyenne des données historiques, constitue la valeur d'alerte de base pour la période de surveillance suivante. Le principe SD (une fonction de base de MS Excel) établit les critères de niveau d'alerte en fonction de la performance historique réelle de l'indicateur considéré (série de données), notamment sa volatilité (fluctuations des points de données). Une série de données historiques plus volatiles donnera des valeurs de niveau d'alerte plus élevées (plus généreuses) pour la prochaine période de surveillance. L'Appendice 4 contient des éléments indicatifs sur l'établissement des niveaux d'alerte à partir des critères SD.

4.3.5.10 Les indicateurs de sécurité de base d'un État (ALoSP initial) sont généralement des indicateurs de sécurité à conséquences élevées, tels les taux d'accident et d'incident grave pour chaque secteur. Il importe d'exprimer normalement ces données en termes de taux plutôt qu'en nombres absolus d'incidents. Par la suite, durant une étape plus tardive de l'ALoSP, des indicateurs de sécurité à conséquences plus faibles pourront alors être établis pour compléter l'ensemble ALoSP. (Les indicateurs à conséquences plus faibles sont parfois appelés des indicateurs « proactifs/prédictifs ».)

4.3.5.11 Une fois que l'ensemble ALoSP d'indicateurs de sécurité, de cibles et de niveaux d'alerte d'un État a été établi, il est alors possible de compiler de façon régulière un résumé des résultats des performances de chacun des indicateurs de sécurité. La cible et le niveau d'alerte de chaque indicateur peuvent ensuite être comparés pour déterminer leur état de performance respectif (réalisation). Un résumé récapitulatif des résultats généraux des performances des cibles et des alertes de l'ensemble complet des indicateurs de sécurité de l'ALoSP peut ensuite être compilé pour une année particulière ou une période de surveillance donnée. Si l'on veut, une valeur quantitative peut aussi être attribuée à chaque « cible atteinte » ou à chaque « niveau d'alerte non dépassé » (points positifs). Cela permet d'avoir une mesure numérique ou en pourcentage de la performance de l'ALoSP. Cette performance pour une année ou une période de surveillance donnée peut être comparée à des performances antérieures ou futures. Les États sont libres de renforcer davantage ces critères de mesure de base des performances de l'ALoSP en y ajoutant s'il y a lieu d'autres facteurs ou d'autres procédures.

4.3.5.12 Pour assurer que les indicateurs de sécurité de l'ALoSP restent effectifs et appropriés avec le temps, il convient de les revoir périodiquement afin de déterminer si des modifications ou des ajouts aux indicateurs, aux cibles et aux alertes existantes sont nécessaires. Cet examen périodique de l'ALoSP et toutes modifications qui en résulteraient peuvent être effectués au niveau de la plate-forme de coordination du PNS, s'il y a lieu. L'Appendice 4 au présent chapitre contient de plus amples informations sur l'établissement des critères régissant les indicateurs de sécurité, les cibles et les niveaux d'alerte. Des éléments indicatifs similaires sur les performances des indicateurs de sécurité des SNS figurent également dans les Chapitres 2 et 5.

4.4 MISE EN ŒUVRE DU PNS — MÉTHODE PAR ÉTAPE

4.4.1 La mise en œuvre du PNS est facilitée par la détermination des processus liés à chacun des quatre composants et des éléments connexes du cadre PNS. La mise en œuvre progressive ou par étape d'un PNS permet de gérer efficacement la charge de travail et les attentes à l'intérieur d'un calendrier réaliste. L'échelonnement effectif ou la priorisation des tâches liées à la mise en œuvre des divers éléments du PNS varieront avec les États. La méthode par étape décrite dans le présent chapitre suppose que les 11 éléments du PNS nécessiteront une certaine mesure de mise en œuvre supplémentaire. Certains de ces éléments ou processus sont déjà bien installés et peuvent donc être intégrés ou liés au cadre du PNS, selon qu'il convient.

4.4.2 Une méthode de mise en œuvre du PNS en quatre phases est décrite dans la présente section. Cette méthode prévoit le réaménagement des 11 éléments du PNS et leur répartition entre les quatre phases. Ce réaménagement vise à faciliter la mise en œuvre progressive des éléments et des processus. Le Tableau 4-1 fait une présentation générale des quatre phases et des éléments.

Phase 1

4.4.3 Responsabilités et imputabilité de l'État en matière de sécurité —Élément 1.2 (i)

- a) Identifier l'organisation signet du PNS et l'administrateur responsable du PNS. Ce dernier devrait disposer au minimum des éléments suivants :
 - 1) autorité et imputabilité, au nom de l'État, pour la mise en œuvre et le maintien du PNS dans tout le système d'aviation, à l'exception de l'organisme d'enquête sur les accidents de l'État ;
 - 2) autorité sur les questions de ressources humaines liées à l'organisation signet du PNS ;
 - 3) autorité sur les questions financières importantes liées à l'organisation signet du PNS ;
 - 4) autorité sur la supervision de la certification et de la sécurité des fournisseurs de services par l'organisation signet du PNS ;
 - 5) responsabilité de la coordination à l'échelle nationale de toutes les questions liées au PNS.
- b) Établir l'équipe de mise en œuvre du PNS. L'équipe devrait se composer de représentants des organismes nationaux compétents de réglementation et d'administration. Il a pour rôle d'assurer la mise en œuvre du PNS depuis la planification jusqu'à l'achèvement. Une fois achevée la mise en œuvre, l'organisation signet du PNS, en collaboration avec le service/bureau responsable de l'administration du PNS, prendrait la relève de l'équipe de mise en œuvre. Les autres fonctions de l'équipe de mise en œuvre devraient inclure, sans s'y limiter :
 - 1) la coordination du processus d'analyse des carences ;
 - 2) l'établissement du plan de mise en œuvre du PNS ;
 - 3) la formation adéquate au PNS et l'expertise technique de l'équipe afin d'établir la réalisation effective des éléments du PNS et des processus connexes ;
 - 4) la surveillance et le compte rendu des progrès de la mise en œuvre du PNS, en soumettant des rapports réguliers de mise à jour, en assurant la coordination avec l'administrateur responsable du PNS et en faisant respecter le calendrier pour les activités des différentes phases.

Assurer l'exécution effective du plan de mise en œuvre, notamment dans le cas des États disposant d'organisations multiples, où l'administrateur responsable devra veiller à ce que l'équipe de mise en œuvre dispose de l'autorité et du soutien nécessaire à la gestion.

Tableau 4-1. Exemple des quatre phases de la mise en œuvre du PNS

<i>Phase 1 (12 mois)</i>	<i>Phase 2 (12 mois)</i>	<i>Phase 3 (24 mois)</i>	<i>Phase 4 (24 mois)</i>
<p>1. Élément 1.2 (i) :</p> <p>a) identifier l'organisation signet et l'administrateur responsable du PNS ;</p> <p>b) établir l'équipe de mise en œuvre du PNS ;</p> <p>c) effectuer une analyse des carences du PNS ;</p> <p>d) établir un plan de mise en œuvre du PNS ;</p> <p>e) établir un mécanisme de coordination du PNS ;</p> <p>f) élaborer la documentation requise du PNS, incluant le cadre national du PNS, ses composants et éléments.</p>	<p>1. Élément 1.1 :</p> <p>Établir un cadre législatif national de la sécurité.</p> <p>2. Élément 1.2 (ii) :</p> <p>a) identifier, définir et documenter la gestion des responsabilités et des imputabilités de la sécurité ;</p> <p>b) définir et documenter les politiques et les objectifs de sécurité de l'État.</p> <p>3. Élément 1.3 :</p> <p>établir une procédure d'enquête sur les accidents et incidents graves.</p> <p>4. Élément 1.4 (i) :</p> <p>Établir une législation d'exécution de base (pénalités).</p> <p>5. Élément 3.1 (i) :</p> <p>Assurer la supervision et la surveillance efficaces des fournisseurs de services.</p> <p>6. Élément 2.1 (i) :</p> <p>Faciliter et promouvoir la formation au SGS des fournisseurs de services.</p>	<p>1. Élément 1.4 (ii) :</p> <p>Promulguer la politique/la législation d'exécution, incluant :</p> <p>a) dispositions relatives aux fournisseurs de services régis par un SGS pour résoudre à l'interne les écarts de sécurité et de qualité ;</p> <p>b) conditions et circonstances dans lesquelles l'État peut intervenir en cas d'écarts de sécurité ;</p> <p>c) dispositions pour prévenir l'utilisation ou la divulgation des données de sécurité à des fins autres que le renforcement de la sécurité ;</p> <p>d) dispositions pour protéger les sources d'information provenant des systèmes de comptes rendus volontaires/confidentiels.</p> <p>2. Élément 2.1 (ii) :</p> <p>Établir des règlements harmonisés imposant la mise en œuvre des SGS.</p> <p>3. Élément 3.2 (i) :</p> <p>a) établir des systèmes de collecte et d'échange de données de sécurité ;</p> <p>b) établir des indicateurs de performance de sécurité et des cibles et des niveaux d'alerte à conséquences élevées.</p>	<p>1. Élément 2.2 :</p> <p>Examiner et approuver les performances des indicateurs de sécurité des fournisseurs de services.</p> <p>2. Élément 3.1 (ii) :</p> <p>Incorporer le SGS du fournisseur de services et les performances des indicateurs de sécurité dans le programme de surveillance de routine.</p> <p>3. Élément 3.2 (ii) :</p> <p>a) mettre en œuvre des systèmes de compte rendu de sécurité volontaire/confidentiels ;</p> <p>b) établir des indicateurs de sécurité/qualité à conséquences plus faibles, avec la surveillance de cibles/de niveaux d'alerte s'il y a lieu ;</p> <p>c) promouvoir l'échange d'informations de sécurité avec et entre les fournisseurs de services et les autres États.</p> <p>4. Élément 3.3 :</p> <p>Prioriser les inspections et les audits en fonction des analyses de risques de sécurité ou des données de qualité, le cas échéant.</p> <p>5. Élément 3.1 (iii)</p> <p>Établir un mécanisme d'examen interne couvrant le PNS pour en assurer l'efficacité et l'amélioration constantes.</p>

Note 1.— Les éléments 4.1 et 4.2 (formation au PNS et au SGS à l'interne ; promotion de la formation au SGS à l'externe ; communication et diffusion internes et externes d'informations de sécurité) sont mis en œuvre progressivement durant les Phases 1 à 4.

Note 2.— La durée de chaque phase (p. ex. 12 mois pour la Phase 1) est approximative. La période réelle de mise en œuvre dépendra de la portée/complexité du système d'aviation de l'État, des carences effectives dans chaque élément et de la structure organisationnelle.

- c) Réaliser une analyse des carences du PNS. Pour établir un plan de mise en œuvre du PNS, il convient d'effectuer une analyse des carences des structures et des procédures existantes dans l'État selon le cadre PNS de l'OACI. Cela permettra à l'État de déterminer l'existence et la maturité des éléments de son PNS. Une fois l'analyse terminée et documentée, les composants/éléments/procédures identifiés comme manquants ou insuffisants, ainsi que les éléments déjà en place, constitueront la base du plan de mise en œuvre du PNS. L'Appendice 7 au présent chapitre contient un exemple de liste de vérification d'une analyse des carences d'un PNS.
- d) Établir un plan de mise en œuvre du PNS. Le plan servira de guide pour l'établissement du PNS et son intégration dans les activités de gestion de la sécurité de l'État. Le plan devrait :
 - 1) établir clairement les activités (éléments/procédures) qui seront entreprises ou achevées selon leurs phases ou dates limites imposées. Ces activités dépendront des résultats de l'analyse des carences ;
 - 2) déterminer un calendrier réaliste, incluant les jalons, pour l'exécution de chaque activité ou phase. Dépendamment de la complexité du PNS, un plan de mise en œuvre du PNS pourrait être compilé comme un simple tableau Word/Excel ou, s'il y a lieu, en utilisant un outil de gestion de projet tel qu'un graphique Gantt. L'Appendice 7 au présent chapitre contient un échantillon/exemple de plan de mise en œuvre de base du PNS.
- e) Établir une plate-forme nationale de coordination de la sécurité aérienne. Entamer, si ce n'est déjà fait, l'établissement d'un mécanisme de coordination du PNS avec la participation de tous les organismes nationaux de réglementation et d'administration de l'aviation. Ce mécanisme peut prendre la forme d'un conseil ou d'un comité. Il aura pour fonction de coordonner la mise en œuvre et l'administration subséquente du PNS entre les différents organismes nationaux de réglementation et d'administration de l'aviation. On assurera ainsi que l'établissement, l'examen périodique et les processus décisionnel et d'établissement de politiques portant sur les activités du PNS, tels que la politique de sécurité, les indicateurs de sécurité, la politique d'exécution, la protection et le partage des données de sécurité, les dispositions réglementaires des SGS, et l'examen interne du PNS et les résultats, sont exécutés de façon intégrée et coordonnée. Une telle plate-forme permanente du PNS devrait avoir la participation des cadres supérieurs des diverses organisations, l'administrateur responsable du PNS assurant les fonctions de coordination.
- f) Établir la documentation du PNS. Le processus d'élaboration d'une documentation du PNS devrait commencer dès le début des activités de mise en œuvre du PNS. Au fur et à mesure de la définition des composants et éléments du PNS, la description de chaque élément et du processus connexe peut être intégrée dans ce document de haut niveau. Voir dans l'Appendice 8 un exemple illustratif de la structure d'un document de PNS et de son contenu. Établir un système de documentation du PNS (bibliothèque/filière/dossier) au sein de l'organisation signet du PNS, qui servira de dépositaire central d'éléments tels que le document du PNS, les SOP connexes, les formulaires, les procès-verbaux des réunions, et les dossiers portant sur la mise en œuvre et le fonctionnement continu du PNS. Ces

documents serviront de registres et de preuves des activités réelles et du fonctionnement continu des différents éléments du PNS. Il se peut que certains registres, tels que les rapports confidentiels ou les rapports d'événements, soient conservés dans un système informatique distinct ou confiés à une autre organisation de réglementation ou d'administration. Dans ce cas, des échantillons ou des extraits peuvent être gardés dans la bibliothèque le cas échéant. Un registre central des documents du PNS devrait permettre de localiser tous les documents pertinents. Un système général de documentation facilitera le suivi, la mise à jour, les renvois et l'audit interne/externe du système.

Phase 2

4.4.4 Cadre législatif national de la sécurité — Élément 1.1

- a) Examiner, élaborer et promulguer, selon les besoins, un cadre législatif national de la sécurité et des règlements particuliers, conformément aux normes nationales et internationales, définissant la manière dont l'État assurera la gestion et la réglementation de la sécurité de l'aviation dans son système d'aviation.
- b) Établir un calendrier pour l'examen périodique de la législation sur la sécurité et des règlements opérationnels particuliers pour en assurer la pertinence et le bien-fondé pour l'État.

4.4.5 Responsabilités et imputabilités de l'État en matière de sécurité — Élément 1.2 (ii)

- a) Définir et établir les responsabilités et imputabilités de gestion de la sécurité des organismes de réglementation respectifs. Le document du PNS devrait comprendre une description ou une illustration de la structure organisationnelle existante et de son intégration des diverses organisations de réglementation et d'administration. Il serait alors possible de renvoyer à des documents d'appui en termes de responsabilités et d'imputabilités des organisations respectives.
- b) Élaborer et mettre en œuvre une politique nationale de sécurité et les moyens nécessaires pour assurer que cette politique est bien comprise, mise en œuvre et observée à tous les niveaux au sein des organismes d'aviation de l'État. L'Appendice 1 au présent chapitre contient des éléments d'orientation sur l'élaboration d'une politique nationale de sécurité.
- c) Établir ou inclure des objectifs nationaux généraux de sécurité conformes à la politique nationale de sécurité. Ces objectifs peuvent être autonomes ou faire partie de la déclaration générale de mission de l'organisation, selon sa complexité et ses rôles. Ces objectifs de sécurité devraient alors être pris en compte durant l'établissement ultérieur des indicateurs de sécurité ALoSP de l'État. Des indicateurs devraient être établis pour servir de critères d'évaluation de l'état de réalisation des objectifs de sécurité.

4.4.6 Enquête sur les accidents et incidents — Élément 1.3

L'État devrait :

- a) veiller à ce que le cadre législatif national inclue des dispositions pour l'établissement d'une procédure indépendante d'enquête sur les accidents et incidents, administrée par un organisme, un service, une commission ou tout autre organe indépendant ;
- b) établir un organisme, un service, une commission ou tout autre organe d'enquête sur les accidents, indépendant de toutes les autres organisations d'aviation de l'État. Dans les États où il n'est peut-être pas pratique d'établir une entité permanente d'enquête sur les accidents, une commission ou un

conseil permanent compétent pourrait être établi pour enquêter sur chaque accident retenu. Ces États peuvent également, comme solution de rechange, envisager d'utiliser les d'un RAIO (voir le Doc 9946) ;

- c) établir des mécanismes pour assurer que la procédure d'enquête ait pour seul but la prévention des accidents et incidents, à l'appui de la gestion de la sécurité dans l'État, et non pas l'attribution de blâme ou de responsabilité.

4.4.7 Politique d'exécution — Élément 1.4 (i)

L'État devrait établir ou assurer l'établissement de dispositions législatives fondamentales aux fins de mesures d'exécution réglementaires (pénalités), incluant la suspension ou la révocation de certificats.

4.4.8 Supervision de la sécurité — Élément 3.1 (i)

L'État devrait établir ou assurer l'établissement d'un programme de base de supervision de la sécurité pour surveiller les fournisseurs de services. Un tel programme inclurait un programme de surveillance qui assurerait la conformité réglementaire des fournisseurs de services durant des opérations de routine qui incluraient, sans s'y limiter :

- a) des inspections d'emplacement, de station ou de produit ;
- b) des audits d'organisations ou de systèmes.

4.4.9 Dispositions de sécurité pour le SGS des fournisseurs de services — Élément 2.1 (i)

- a) S'il y a lieu, durant la phase de formation et de promotion de la mise en œuvre du SGS, l'État devrait préparer les fournisseurs de services et les parties prenantes de l'industrie aux dispositions de mise en œuvre par des activités d'information et de promotion, telles que des forums, des séminaires, des briefings ou des ateliers sur le SGS.
- b) Élaborer des éléments d'orientation sur les SGS, pertinents aux fournisseurs de services, en anticipation ou en conjonction avec l'établissement de réglementations sur les SGS. Voir dans l'Appendice 9 au présent chapitre un exemple de règlement national sur les SGS.

Phase 3

4.4.10 Politique d'exécution — Élément 1.4 (ii)

Dans un environnement PNS-SGS, les politiques et procédures d'exécution de l'État devraient établir :

- a) les conditions et les circonstances dans lesquelles les fournisseurs de services sont autorisés à traiter et à résoudre à l'interne des événements comprenant certains écarts de sécurité, dans le contexte du système de gestion de la sécurité (SGS) des fournisseurs de services, à la satisfaction de l'autorité compétente de l'État ;
- b) les conditions et les circonstances dans lesquelles les écarts de sécurité sont traités dans le cadre des procédures d'exécution établies ;

- c) des procédures pour prévenir l'utilisation à des fins d'exécution de toutes informations obtenues des systèmes de compte rendu volontaires/confidentiels ou des systèmes équivalents de surveillance de données opérationnels restreintes fonctionnant dans le cadre d'un SGS ;
- d) une procédure pour protéger les sources d'informations obtenues de systèmes de compte rendu volontaires ou confidentiels.

L'Appendice 10 au présent chapitre présente un exemple de politique nationale d'exécution tandis que l'Appendice 11 contient des exemples de procédures nationales d'exécution.

4.4.11 Dispositions de SGS applicables aux fournisseurs de services — Élément 2.1 (ii)

- a) Établir des règlements, des éléments indicatifs et des dispositions d'exécution sur les SGS à l'intention de tous les fournisseurs de services intéressés et veiller à l'harmonisation du cadre de réglementation des SGS dans tous les secteurs de l'aviation, et à sa compatibilité avec le cadre SGS de l'OACI. L'adoption du cadre harmonisé SGS de l'OACI facilitera la reconnaissance mutuelle entre les États.
- b) Établir une procédure pour l'acceptation du SGS d'un fournisseur de services donné, afin d'assurer que le cadre de son SGS est conforme au cadre réglementaire SGS de l'État. Cette procédure d'examen et d'acceptation initiale peut se manifester par l'approbation ou l'acceptation du manuel SGS de l'organisation. Si l'État a adopté une méthode de mise en œuvre par étape des SGS, la procédure d'acceptation peut être appliquée par étape, selon le cas. Voir à cet égard l'Appendice 12 pour un exemple de liste de vérification d'une évaluation/d'acceptation réglementaire de SGS.

Note.— L'acceptation ou la reconnaissance du SGS d'une organisation étrangère (p. ex. AMO étrangère) est encouragée dans le cas où un SGS a été dûment accepté par l'autorité locale de cette organisation et où le cadre SGS de l'organisation est conforme au cadre SGS de l'OACI.

4.4.12 Collecte, analyse et échange de données de sécurité — Élément 3.2 (i)

L'État devrait :

- a) établir des mécanismes et des procédures pour la collecte et l'analyse des événements à comptes rendus obligatoires ou recommandés au niveau global de l'État. Cela signifie que l'État devra :
 - 1) établir une procédure de compte rendu obligatoire ou recommandé d'événements à l'intention des fournisseurs de services approuvés/certifiés dans chaque secteur de l'aviation aux fins de compte rendu (obligatoire) d'accidents et d'incidents graves. La procédure devrait inclure des rapports de défauts importants ou des rapports obligatoires de défauts (MDR), selon le cas. L'Appendice 3 contient un exemple de procédure de compte rendu obligatoire ;
 - 2) établir des dispositions forçant les fournisseurs de services à avoir en place des procédures internes d'enquête et de résolution d'événements, documentant les résultats des enquêtes et mettant les rapports à la disposition des organismes de réglementation respectifs ;
 - 3) assurer que les données recueillies des divers secteurs aéronautiques sont bien intégrées, regroupées et rassemblées au niveau du PNS. Les données de sécurité ne devraient pas exister dans des bases de données indépendantes ou autonomes, au niveau sectoriel. L'aspect d'intégration doit également être souligné dans les bases de données respectives de l'AAC et des autorités d'enquête indépendantes, notamment dans le cas des États où certaines fonctions de gestion de la sécurité sont confiées à une RSOO ou une RAIO agissant au nom de ces États ;

- b) établir des indicateurs de sécurité de base à conséquences élevées (ALoSP initial) et leurs cibles et niveaux d'alerte correspondants. Ces indicateurs à conséquences élevées peuvent être, par exemple des taux d'accident, des taux d'incident grave et des résultats de la surveillance de cas de risques élevés, d'application de règlements ou de cas de non-conformité (p. ex. résultats d'audits OACI). L'établissement et la sélection d'indicateurs de sécurité devraient être conformes aux objectifs nationaux et aux politiques nationales de sécurité. Ils doivent être appropriés et pertinents à l'ampleur et à la complexité des activités aéronautiques de l'État. La sélection d'indicateurs de sécurité à conséquences plus faibles peut être abordée ultérieurement. Les indicateurs de sécurité seront surveillés périodiquement, pour éliminer toutes tendances indésirables et tous dépassements des niveaux d'alerte et pour réaliser les objectifs visés. L'Appendice 4 contient des directives pour l'établissement et la surveillance d'indicateurs de sécurité.

Phase 4

4.4.13 Accord sur les performances de sécurité du fournisseur de services — Élément 2.2

L'État devrait établir une procédure de liaison avec les fournisseurs de services en vue de l'établissement d'une série d'indicateurs de performances de sécurité (SPI), de cibles et de niveaux d'alerte réalistes, dans la mesure du possible, selon l'ampleur et la complexité de l'Organisation. Les indicateurs de sécurité, les cibles et les alertes devraient être :

- a) une combinaison de SPI à conséquences élevées ou faibles, selon le cas ;
- b) pertinents aux activités aéronautiques du fournisseur de services ;
- c) cohérents avec les autres fournisseurs de services du même secteur ou de la même catégorie ;
- d) compatibles avec les indicateurs de sécurité globaux du PNS établis par l'État pour le secteur ou la catégorie du fournisseur de services.

Une fois établis les indicateurs de sécurité, les cibles et les alertes, les fournisseurs de service devront documenter leurs plans d'action en fonction du degré d'achèvement des cibles et leurs plans d'action correctrice au cas où un niveau d'alerte est dépassé. En établissant les exigences de performance, l'organisme de réglementation devra présenter de façon transparente la procédure d'examen périodique des performances de sécurité des fournisseurs de services qui sera appliquée.

4.4.14 Supervision de la sécurité — Élément 3.1 (ii)

L'État devrait incorporer la supervision des SGS des fournisseurs de services dans son programme de surveillance de routine, qui inclura les mesures suivantes :

- a) organiser, de concert avec les fournisseurs de services, des examens périodiques des spécifications des SGS et des éléments indicatifs connexes pour en assurer la pertinence et le bien-fondé ;
- b) mesurer les performances de sécurité des SGS des différents fournisseurs de services par des examens périodiques des performances de sécurité convenues et assurer que les SPI, les cibles et les alertes restent pertinentes aux fournisseurs de services ;

- c) assurer que les procédures d'identification des dangers et de gestion des risques de sécurité des fournisseurs de services répondent aux exigences réglementaires établies et que les mesures de contrôle des risques de sécurité sont intégrées comme il faut dans les SGS des fournisseurs de services.

4.4.15 Supervision de la sécurité — Élément 3.1 (iii)

L'État devrait établir un mécanisme interne d'examen ou d'évaluation couvrant le PNS et sa politique de sécurité pour assurer la conformité et l'amélioration continues du PNS. À l'instar de tout mécanisme interne efficace, le processus d'examen doit disposer d'un degré approprié d'indépendance et d'imputabilité dans le suivi.

4.4.16 Collecte, analyse et échange de données de sécurité — Élément 3.2 (ii)

L'État devrait :

- a) établir à l'échelle nationale un système de compte rendu volontaire, incluant des dispositions de protection des informations de sécurité. Voir l'Appendice 5 pour des directives sur la protection des informations de sécurité. Ce système de compte rendu volontaire devrait faire partie du système de collecte et de traitement de données de sécurité du PNS. La base de données de ce système volontaire devrait faire partie du SDCPS du PNS et être accessible à l'AAC de l'État, ainsi qu'aux services d'enquête sur les accidents. Voir l'Appendice 2 pour des directives sur les systèmes nationaux de compte rendu volontaires ;
- b) établir des indicateurs de sécurité et/ou de qualité de sécurité à faibles conséquences avec la surveillance appropriée des cibles et des alertes (ALoSP mûr). La sélection et le développement d'indicateurs de sécurité devraient être conformes aux objectifs et aux politiques de sécurité de l'État, aussi bien qu'appropriés et pertinents à la portée et à la complexité des activités aéronautiques de l'État. Une surveillance périodique des indicateurs de sécurité est recommandée pour détecter toutes tendances non voulues, tous dépassements des niveaux, ainsi que la réalisation des cibles. Voir l'Appendice 4 pour des directives sur l'établissement et la surveillance des indicateurs de sécurité ;
- c) promouvoir l'échange et le partage d'informations de sécurité entre les organismes nationaux de réglementation et d'administration et les fournisseurs de services, ainsi qu'avec d'autres États et organisations de l'industrie.

4.4.17 Ciblage fondé sur les données de sécurité pour la supervision de domaines présentant plus de problèmes ou de besoins — Élément 3.3

L'État devrait revoir les programmes existants de surveillance et d'audit afin d'y incorporer des dispositions sur l'étalonnage de la fréquence et de la portée des activités de surveillance ou d'audit des différents fournisseurs de services, en fonction des résultats des performances pertinents et des données de sécurité introduites. Voir la Section 4.2, Élément 3.3, 4.2.36 et 4.2.37 du PNS pour des directives sur le concept de surveillance fondé sur les données de sécurité.

4.4.18 Formation, communication et diffusion internes des informations de sécurité — Élément 4.1 (Phases 1 à 4)

L'État devrait :

- a) élaborer des politiques et des procédures de formation interne ;

- b) mettre sur pied un programme de formation aux PNS et SGS à l'intention du personnel compétent. La priorité serait accordée au personnel chargé de la mise en œuvre des PNS-SGS et aux inspecteurs opérationnels/sur le terrain chargés de couvrir les SGS des fournisseurs de services ;
- c) inclure des procédures propres au PNS national et leur pertinence aux éléments du cadre générique de l'OACI dans les textes et matériaux de formation ultérieure à la mise en œuvre des PNS et SGS ;
- d) établir un moyen de communiquer des informations liées à la sécurité, notamment des documents sur le PNS national et les politiques et procédures de sécurité et d'application, aux organisations de réglementation et d'administration de l'État, au moyen de mécanismes tels que circulaires, bulletins et sites web.

4.4.19 Formation, communication et diffusion externes des informations de sécurité — Élément 4.2 (Phases 1 à 4)

L'État devrait :

- a) établir une procédure pour communiquer aux fournisseurs de services des informations réglementaires liées aux PNS et SGS ;
- b) élaborer, à l'intention des fournisseurs de services, des éléments d'orientation sur la mise en œuvre des SGS ;
- c) établir les moyens de communiquer à l'extérieur des informations sur les questions de sécurité, notamment les politiques et les procédures liées à la sécurité, au moyen de mécanismes tels que circulaires, bulletins et sites web ;
- d) promouvoir l'échange d'informations de sécurité avec et entre les fournisseurs de services et les autres États ;
- e) faciliter la formation et la familiarisation des fournisseurs de services concernant les SGS, s'il y a lieu.

Note.— Les éléments 4.4.18 et 4.4.19 sont élaborés et mis en œuvre progressivement, durant toutes les phases de mise en œuvre.

Appendice 1 au Chapitre 4

DIRECTIVES SUR L'ÉTABLISSEMENT D'UN ÉNONCÉ DE POLITIQUE NATIONALE SUR LA SÉCURITÉ

1. GÉNÉRALITÉS

1.1 L'énoncé de politique nationale sur la sécurité devrait couvrir, sans nécessairement s'y limiter, les engagements ci-après :

- a) établir et mettre en œuvre des stratégies et des procédures pour assurer que toutes les activités et opérations aéronautiques réaliseront le plus haut niveau de performances de sécurité ;
- b) établir et promulguer un cadre législatif national de sécurité et des règlements d'exploitation applicables en vue de la gestion de la sécurité dans l'État, fondée sur une analyse approfondie du système de l'aviation de l'État, qui respecte, voire, dans la mesure du possible, dépasse les exigences et les normes internationales de sécurité ;
- c) consulter les segments pertinents de l'industrie de l'aviation sur des questions liées à l'établissement de règlements ;
- d) affecter les ressources nécessaires aux organisations aéronautiques nationales pour assurer que le personnel reçoive la formation adéquate et qu'il puisse s'acquitter de ses responsabilités ;
- e) appuyer la gestion de la sécurité par la promotion de systèmes de comptes rendus volontaires et confidentiels au niveau des fournisseurs de services aussi bien qu'au niveau de l'État ;
- f) mener des activités de supervision axées sur les données, fondées sur les risques et priorisées, fondées sur les performances et axées sur la conformité ; et assurer que ces activités de supervision réglementaires et administratives sont menées conformément aux normes internationales et aux meilleures pratiques, le cas échéant ;
- g) promouvoir et éduquer l'industrie de l'aviation sur les concepts et les principes de la gestion de la sécurité et superviser la mise en œuvre et l'exécution des SGS par les fournisseurs de services de l'État ;
- h) établir des dispositions pour la protection des systèmes de collecte et de traitement des données de sécurité, afin d'encourager le personnel et les organisations à fournir les informations essentielles de sécurité, et d'assurer le flot et l'échange continu de données de gestion de la sécurité entre l'État et les fournisseurs de services ;
- i) assurer une interaction efficace avec les fournisseurs de services dans la résolution des problèmes de sécurité ;

- j) maintenir une politique et des procédures d'application en complément à la protection des informations découlant des systèmes de collecte et de traitement des données de sécurité ;
- k) établir un mécanisme de surveillance et de mesure des performances du PNS au moyen d'indicateurs de sécurité et de leurs cibles et niveaux d'alertes correspondants ;
- l) promouvoir l'adoption des meilleures pratiques et une culture positive de la sécurité chez les organisations de fournisseurs de services.

1.2 L'énoncé de politique nationale sur la sécurité devrait être signé par l'administrateur responsable du PNS ou un fonctionnaire des services compétents de l'État responsables de la supervision des instances de réglementation et d'administration de l'État.

2. MODÈLE D'ÉNONCÉ DE BASE DE POLITIQUE SUR LA SÉCURITÉ

Le texte ci-après est un modèle d'énoncé de base de politique sur la sécurité :

[Nom de l'organisme de réglementation de l'État] promeut et réglemente la sécurité de l'aviation au [Nom de l'État]. Nous sommes déterminés à établir et à mettre en œuvre des stratégies efficaces, des cadres de réglementation et des procédures afin d'assurer que les activités de l'aviation placées sous notre supervision atteignent le plus haut niveau possible de sécurité.

À cette fin, nous nous engageons :

- 1) à établir des normes nationales conformes aux Normes, aux Pratiques recommandées et aux Procédures de l'Organisation de l'aviation civile internationale ;
- 2) à adopter une approche axée sur les données et fondée sur les performances dans l'exécution des activités de réglementation de la sécurité et de supervision de l'industrie, comme il convient ;
- 3) à identifier les tendances en matière de sécurité au sein du milieu de l'aviation et à adopter une démarche fondée sur les risques pour aborder les domaines présentant le plus de problèmes ou de besoins ;
- 4) à surveiller et à mesurer de façon continue les performances de sécurité de notre système de l'aviation, au moyen d'indicateurs globaux de sécurité de l'État, ainsi que des performances des indicateurs de sécurité des fournisseurs de services ;
- 5) à consulter et à collaborer avec l'industrie de l'aviation pour résoudre les questions de sécurité et renforcer de façon continue la sécurité de l'aviation ;
- 6) à promouvoir au sein de l'industrie les bonnes pratiques et une culture positive de la sécurité fondée sur des principes solides de gestion de la sécurité ;
- 7) à encourager la collecte, l'analyse et l'échange d'informations de sécurité parmi toutes les organisations compétentes de l'industrie et les fournisseurs de services, de façon que ces informations ne servent strictement qu'à la gestion de la sécurité ;
- 8) à affecter des ressources financières et humaines suffisantes pour la gestion et la supervision de la sécurité ;

- 9) à doter le personnel des aptitudes et des compétences requises pour lui permettre de s'acquitter de façon effective de ses fonctions et de ses responsabilités de supervision et de gestion.

(Signé)

DGCA [administrateur responsable du
PNS ou fonctionnaire des services de
l'État responsables de l'aviation civile]

Appendice 2 au Chapitre 4

DIRECTIVES SUR UN SYSTÈME NATIONAL DE COMPTE RENDU VOLONTAIRE ET CONFIDENTIEL

[Voir l'Élément 3.2 du PNS et le Chapitre 4, 4.4.16 a)]

Un système national de compte rendu volontaire et confidentiel devait, à tout le moins, définir/indiquer les éléments suivants :

- a) l'objectif du système de compte rendu ;

Exemple :

Le système de compte rendu volontaire et confidentiel de [nom de l'État] a pour objectif principal de renforcer la sécurité de l'aviation par la collecte de rapports sur les carences réelles ou potentielles de sécurité qui ne seraient autrement pas signalées par d'autres voies. Ces rapports peuvent couvrir des incidents, des dangers ou des menaces liés à la sécurité aérienne. Un tel système n'élimine pas la nécessité de soumettre des rapports obligatoires d'accidents et incidents d'aviation aux autorités compétentes conformément aux règlements aéronautiques en vigueur. Les auteurs de comptes rendus sont encouragés à utiliser, le cas échéant, le système de compte rendu volontaire du SGS interne de leurs organisations, à moins qu'ils n'aient pas accès à un tel système ou si l'incident ou le danger est considéré comme dépassant le ressort de leur organisation.

Le [Nom du système] est un système de compte rendu volontaire, non punitif, confidentiel établi par [Nom de l'organisation de réglementation/d'administration]. Il constitue une voie pour le signalement volontaire d'incidents ou de dangers d'aviation tout en protégeant l'identité de l'auteur du compte rendu.

- b) la portée des secteurs/domaines de l'aviation couverts par le système ;

Exemple :

Le [nom du système] couvre des domaines tels que :

- a) Opérations aériennes :
- i) départ/en route/approche et atterrissage ;
 - ii) opérations de cabine d'aéronef ;
 - iii) incidents de proximité en vol ;
 - iv) poids et équilibre et performances.

- b) Opérations d'aérodrome :
 - i) mouvements d'aéronefs au sol ;
 - ii) mouvements sur l'aérodrome ;
 - iii) avitaillement en carburant ;
 - iv) entretiens ou services à l'aérodrome ;
 - v) chargement de marchandises.
- c) Gestion de la circulation aérienne :
 - i) Opérations ATC ;
 - ii) Équipement ATC et aides de navigation ;
 - iii) Communications équipage et ATC.
- d) Maintenance d'aéronefs :
 - i) Activités de maintenance et de réparation d'aéronef/moteur/élément.
- e) Conception et fabrication :
 - i) Activités de conception et de fabrication d'aéronefs/moteurs/éléments.
- f) Institutions de formation approuvées :
 - i) activités de formation couvrant des opérations aériennes.
- g) Divers :
 - i) Traitement de passagers lié à la sécurité ;
 - ii) etc.

- c) qui peut faire un rapport volontaire ;

Exemple :

Les personnes appartenant aux groupes ci-après peuvent contribuer au renforcement de la sécurité de l'aviation par l'intermédiaire de [nom du système] en soumettant des rapports sur des incidents, des dangers ou des menaces dans le système de l'aviation :

- a) membres d'équipage de conduite et d'équipage de cabine ;
- b) contrôleurs de la circulation aérienne ;
- c) techniciens d'entretien ou mécaniciens d'aéronef ;
- d) personnel d'organismes de maintenance, de dessin ou de fabrication ;
- e) exploitants de services d'escale aux aérodromes ;

- f) personnel d'aérodromes ;
- g) personnel d'aviation générale ;
- h) etc.

d) quand faut-il faire un tel rapport ;

Exemple :

Il faut faire un rapport dans les circonstances suivantes :

- a) vous voulez que d'autres apprennent et tirent parti de l'incident ou du danger signalé, mais vous tenez à protéger votre identité ;
- b) il n'existe aucune autre procédure ou voie appropriée pour faire un rapport ;
- c) vous avez essayé une autre procédure ou voie de compte rendu, sans que le problème ne soit résolu.

e) comment les rapports sont traités ;

Exemple :

Le [Nom du système] accorde une attention particulière à la nécessité de protéger l'identité des auteurs de comptes rendus durant le traitement de tous les rapports. Chaque rapport est lu et validé par l'administrateur. Celui-ci peut contacter l'auteur pour s'assurer de bien comprendre la nature et les circonstances de l'incident ou du danger signalé et/ou pour obtenir les informations et explications supplémentaires nécessaires.

Une fois qu'il est convaincu que les informations obtenues sont complètes et cohérentes, l'administrateur éliminera tout élément identificateur des informations et introduira les données dans la base de données du [Nom du système]. Si des contributions de tierces parties sont requises, seules des informations sans identification seront utilisées.

Le formulaire du [Nom du système], portant la date de retour, sera à terme renvoyé à l'auteur du compte rendu. L'administrateur s'efforcera de terminer la procédure dans un délai de dix (10) jours ouvrables, si aucun renseignement supplémentaire n'est requis. Le délai peut être plus long si l'administrateur doit discuter du cas avec l'auteur ou consulter une tierce partie.

En cas d'une absence prolongée de l'administrateur, l'administrateur suppléant assurera le traitement du rapport. Les auteurs des rapports peuvent être assurés que tous les rapports du [Nom du système] seront lus et suivis par l'administrateur ou son suppléant.

Rétroaction de la communauté aéronautique

Les rapports pertinents sans identification et les extraits peuvent être partagés avec la communauté aéronautique dans des publications périodiques, pour que tous puissent tirer des leçons des expériences. Les autorités compétentes et les parties intéressées peuvent également revoir leurs politiques et leurs plans aux fins d'améliorations.

Si le contenu d'un rapport du [Nom du système] laisse penser qu'une situation ou une condition pose une menace immédiate ou urgente à la sécurité de l'aviation, ce rapport sera traité en priorité et renvoyé le plus tôt possible, après l'élimination de tout élément d'identification, aux organisations compétentes pour qu'elles puissent prendre les mesures de sécurité nécessaires.

f) comment contacter l'administrateur du [Nom du système] ;

Exemple :

Vous pouvez toujours appeler [Nom de l'organisation de réglementation/d'administration] pour vous enquérir du [Nom du système] ou pour demander un premier entretien avec l'administrateur du [Nom du système] avant de soumettre un rapport. L'administrateur et son suppléant peuvent être rejoints durant les heures de bureau du lundi au vendredi aux numéros de téléphone suivants :

Administrateur du [Nom du système]

M. ABC

Tél. :

Administrateur suppléant

M. XYZ

Tél. :

Appendice 3 au Chapitre 4

EXEMPLE DE PROCÉDURE NATIONALE DE COMPTE RENDU OBLIGATOIRE

Les paragraphes qui suivent décrivent un modèle de procédure nationale de compte rendu obligatoire, couvrant les systèmes de compte rendu obligatoire d'incidents. Cette procédure concerne les rapports obligatoires et en temps opportun d'accidents, d'incidents graves, d'incidents et autres événements devant être signalés par les parties intéressées. Selon le règlement de l'État, ces parties prenantes peuvent être des organismes aéronautiques certifiés/agrétés, des employés homologués/autorisés indépendants (tels que les pilotes, les équipages de cabine, les contrôleurs de la circulation aérienne, le personnel d'entretien) et les membres du public.

Note 1.— Si un État le préfère, le compte rendu obligatoire d'accidents et d'incidents graves, et celui des défaillances/défectuosités/difficultés en service, etc., peuvent être couverts par des procédures distinctes ; autrement, ils peuvent être couverts par la procédure de compte rendu obligatoire (dans cet exemple illustré, par exemple).

Note 2.— Dans certains cas, une « remarque » est incluse entre crochets []. Il s'agit d'une directive administrative à l'intention des États lorsqu'ils établiront leur propre procédure de compte rendu obligatoire.

1. COMPTE RENDU OBLIGATOIRE

1.1 Conformément à [règlement(s)], les [noms des parties intéressées] doivent obligatoirement signaler les accidents d'aviation, incidents graves, incidents et autres événements liés à la sécurité (incluant les défaillances/défectuosités/difficultés en service) à [Nom de l'Autorité/agence/service].

1.2 La liste d'événements devant être signalés (outre les accidents) et les calendriers de compte rendu figurent à l'Annexe A à la présente procédure. [*Remarque* : Bien que l'Annexe A contient essentiellement des exemples d'incidents graves, les États sont invités à inclure d'autres événements devant faire l'objet de rapports dans le cadre de ce système de compte rendu obligatoire.]

1.3 Le compte rendu obligatoire d'un événement se fait par le Rapport obligatoire [Formulaire XYZ]. Tous les rapports obligatoires sont signés par le signataire autorisé de l'organisme approuvé/homologué, le cas échéant. [*Remarque* : Il conviendrait d'établir également une procédure pour couvrir les notifications reçues par communications verbales ou téléphoniques.]

1.4 Dans le cas d'accidents et d'incidents graves, il convient d'entamer immédiatement une coordination avec [Nom de l'autorité nationale d'enquête sur les accidents], à la réception de la notification, afin de déterminer la nécessité de lancer un processus d'enquête indépendante. [*Remarque* : Le processus réel de notification et de compte rendu à l'AAC de l'État et/ou à l'autorité d'enquête sur les accidents dépendra de la nature des dispositions et des arrangements de compte rendu obligatoire de l'État. Ces détails particuliers devront alors être pris en compte dans la présente section de la procédure.]

2. TRAITEMENT DES RAPPORTS OBLIGATOIRES

2.1 Dès qu'un rapport obligatoire est reçu, il sera validé pour assurer que toutes les informations essentielles ont bien été fournies par l'auteur.

2.2 Le rapport sera ensuite classé dans les catégories suivantes :

- a) accident ;
- b) incident grave ;
- c) incident ;
- d) autre événement.

2.3 Une fois classé, le rapport sera téléchargé dans la base de données appropriée avec un numéro de référence attribué.

2.4 La situation de chaque rapport sera catégorisée et mise à jour comme suit :

- a) Notification initiale : Évaluation/Suivi/information selon les notes portées.
- b) Sous enquête : Enquête en cours, menée par [Autorité d'enquête sur les accidents/AAC/fournisseur de services], selon les notes portées.
- c) Enquête terminée : Les résultats/données de l'enquête sont reçus et téléchargés.
- d) Dossier clos : Aucune autre mesure n'est requise.

Note.— La notification et la soumission des rapports et des données sur les accidents et incidents graves à l'OACI relèvent de la responsabilité de [Nom de l'autorité d'enquête sur les accidents].

[Remarque : Les États disposant d'autorités multiples ayant des responsabilités de réglementation de la sécurité (telles que l'AAC, l'autorité d'enquête sur les accidents) devraient établir la coordination et l'accès appropriés à la base de données.]

3. CLASSIFICATION DES ACCIDENTS/INCIDENTS GRAVES/INCIDENTS

3.1 La classification des accidents, incidents graves et autres incidents sera fondée sur les définitions de l'Annexe 13 de l'OACI.

3.2 Les événements classés comme des accidents ou des incidents graves peuvent requérir une enquête indépendante par [Nom de l'autorité d'enquête sur les accidents]. Dans ce cas, le représentant désigné de l'AAC suivra les résultats de l'enquête indépendante et fournira s'il y a lieu des mises à jour à [Nom de la base de données de l'AAC].

3.3 Dans le cas d'incidents et autres événements (incluant les défaillances/défectuosités/difficultés en service) qui ne sont pas couverts par le processus d'enquête indépendante de l'État, le représentant désigné de l'AAC assurera la liaison nécessaire avec la partie compétente aux fins de l'enquête de suivi requise et de la soumission de rapport s'il y a lieu.

4. SUIVI/ENQUÊTE

4.1 Dans le cas d'événements qui appellent des mesures de suivi ou une enquête par les services internes de sécurité ou de vérification de qualité des fournisseurs de services, le représentant responsable de l'AAC maintiendra la liaison avec le représentant autorisé des services internes du fournisseur de services afin d'assurer le suivi et la clôture du dossier, selon les besoins.

4.2 Le représentant désigné de l'AAC assure la surveillance et détermine si l'intervention de l'AAC est requise avant, durant ou après l'enquête et la résolution de l'événement par les services internes du fournisseur de services.

4.3 Sur réception du rapport d'enquête/de suivi, le représentant de l'AAC inscrit toutes les informations pertinentes dans la base de données pertinente. S'il s'agit de rapports d'enquête de [Nom de l'autorité d'enquête sur les accidents], le représentant de l'AAC entre en liaison avec cette autorité aux fins de téléchargement des données dans la base de données.

4.4 S'il est jugé nécessaire pour l'AAC de prendre des mesures administratives (d'exécution) à la suite des conclusions d'un rapport d'enquête, des recommandations dans ce sens sont communiquées par l'inspecteur compétent à la DGCA, pour approbation conformément aux procédures d'exécution de l'AAC (Référence xxx). Dans le cas de rapports d'enquête de [Nom de l'autorité d'enquête sur les accidents], il sera dûment tenu compte de l'objectif de l'enquête, énoncé dans l'Annexe 13.

ANNEXE A

I^{re} PARTIE. CALENDRIER DE COMPTE RENDU (EXEMPLE)

	<i>Notification à l'AAC et/ou l'autorité d'enquête sur les accidents*</i>	<i>Soumission obligatoire du rapport (Formulaire XYZ) à l'AAC et/ou l'autorité d'enquête sur les accidents**</i>	<i>Rapport d'enquête à l'AAC***</i>
Accident	Immédiatement/ASAP	Dans les 24 heures	90 jours
Incident grave	Immédiatement/ASAP	Dans les 48 heures	60 jours
Incident	N/A	Dans les 72 heures	30 jours (s'il y a lieu)
<p>* Dans la plupart des cas, le téléphone, le fax ou le courrier électronique constitueront les moyens les plus appropriés et les plus rapides pour l'envoi de la notification.</p> <p>** Cette colonne ne s'applique pas aux membres du public.</p> <p>*** Cette colonne ne s'applique pas aux rapports d'enquête de l'autorité nationale d'enquête sur les accidents.</p>			

II^e PARTIE. EXEMPLES D'ÉVÉNEMENTS DEVANT FAIRE L'OBJET DE COMPTES RENDUS

Note.— La liste ci-après n'est pas exhaustive et n'inclut pas les accidents.

Exploitant aérien

- quasi-abordages nécessitant une manœuvre d'évitement pour éviter une collision ou une situation dangereuse, ou lorsqu'une mesure d'évitement aurait été appropriée ;
- impacts sans perte de contrôle évités de justesse ;
- décollages interrompus sur une piste fermée ou occupée, sur une voie de circulation¹ ou sur une piste non attribuée ;
- décollages à partir d'une piste fermée ou occupée, d'une voie de circulation¹ ou d'une piste non attribuée ;
- atterrissages ou tentatives d'atterrissage sur une piste fermée ou occupée, sur une voie de circulation¹ ou sur une piste non attribuée ;
- incapacité évidente de réaliser les performances prévues durant le décollage ou la montée initiale ;
- incendie et fumée dans la cabine de passagers ou dans la soute de cargo ou incendie moteur, même si le feu est éteint par l'application d'agents extincteurs ;
- incidents nécessitant l'utilisation d'urgence d'oxygène par le personnel navigant ;
- défaillances structurales de l'aéronef ou désintégration des moteurs, incluant les pannes de turbomoteurs non confinées, non classées comme accident ;
- défauts multiples d'un ou de plusieurs systèmes d'aéronef affectant sérieusement le fonctionnement de l'aéronef ;
- incapacité de l'équipage de conduite durant le vol ;
- niveau de carburant nécessitant la déclaration d'une urgence par le pilote ;
- incursions sur piste présentant un niveau de gravité A. Le *Manuel sur la prévention des incursions sur piste* (Doc 9870) contient des informations sur la classification de la gravité ;
- incidents durant le décollage ou l'atterrissage, tels qu'une présentation trop courte, un dépassement de piste ou une sortie latérale de piste ;
- défaillances de système, phénomènes météorologiques, dépassement du domaine de vol approuvé ou autres incidents pouvant entraîner des problèmes de contrôle de l'aéronef ;
- défaillances de plusieurs systèmes dans un système de redondance obligatoire pour le guidage et la navigation ;

1. Excluant les vols autorisés d'hélicoptères.

- [Remarque : Inclure tous autres incidents ou événements considérés par l'État comme devant faire l'objet de rapport en vertu de ce système de comptes rendus obligatoires.]

Organisme d'entretien

- tous défaillances/défectuosités/défauts de cellules, moteurs, hélices, éléments ou systèmes détectés durant les activités régulières ou irrégulières de maintenance d'aéronef (cellule/moteurs/éléments) et pouvant causer un accident ou un incident grave d'exploitation (s'ils ne sont pas corrigés rapidement) ;
- [Remarque : Inclure tous autres incidents ou événements considérés par l'État comme devant faire l'objet de rapport en vertu de ce système de comptes rendus obligatoires.]

Organismes de conception et de fabrication

- tous défaillances/défectuosités/défauts, liés à la conception ou à la fabrication, de produits ou de services détectés ou portés à l'attention de l'organisme de conception ou de fabrication, qui sont considérés comme justifiant la publication possible d'une consigne de navigabilité urgente (CNU), d'une consigne de navigabilité (CN) ou d'un bulletin service d'alerte (BSA) ;
- [Remarque : Inclure tous autres incidents ou événements considérés par l'État comme devant faire l'objet de rapport en vertu de ce système de comptes rendus obligatoires.]

Exploitant d'aérodrome

- incursion sur piste (sans intervention de l'ATC) ;
- sortie/dépassement de piste (sans intervention de l'ATC) ;
- panne ou défaillance grave du balisage lumineux d'aérodrome ;
- dégât occasionné à l'aéronef ou aux moteurs résultant de l'ingestion ou de contact avec des corps étrangers ou des débris sur la piste ou la voie de circulation ;
- incidents dans le périmètre de l'aérodrome causant des dégâts à l'aéronef ou présentant des risques potentiels pour la sécurité des mouvements de l'aéronef au sol ;
- [Remarque : Inclure tous autres incidents ou événements considérés par l'État comme devant faire l'objet de rapport en vertu de ce système de comptes rendus obligatoires.]

Fournisseur ANS/CNS

- tous défaillances/défectuosités/défauts d'équipement ou de système ANS/CNS détectés durant le fonctionnement ou l'entretien de l'équipement qui risquent de causer un accident ou un incident grave d'exploitation ;
- pénétration non autorisée dans l'espace aérien ;
- aéronef près de subir un CFIT ;

- niveau élevé d'incidents ;
- incidents de perte de séparation ;
- incursion en piste (avec communications ATC) ;
- sortie/dépassement de piste (avec communications ATC) ;
- tous autres défaillances/défectuosités/défauts liés à l'ANS, signalés à l'exploitant ANS/CNS et vérifiés par lui, et qui sont considérés comme ayant un impact sur la sécurité de la navigation aérienne ;
- [*Remarque* : Inclure tous autres incidents ou événements considérés par l'État comme devant faire l'objet de rapport en vertu de ce système de comptes rendus obligatoires.]

Note.— Si un État dispose d'autres systèmes de compte rendu obligatoires particuliers propres à un secteur ou à un fournisseur de services, conformes par exemple aux dispositions de l'Annexe 8, Partie II, 4.2.3 f) et 4.2.4 (rapport de maintien de la navigabilité), la corrélation ou l'intégration nécessaire avec la procédure nationale de compte rendu obligatoire liée au PNS devra être apportée, selon les cas.

Appendice 4 au Chapitre 4

INDICATEURS DE PERFORMANCE DE SÉCURITÉ DU PNS

1. Les Tableaux 4-A4-1 à 4-A4-4 (exemples d'indicateurs de sécurité) contiennent des exemples illustratifs d'indicateurs de performance de sécurité (SPI) globaux de l'État et des critères d'établissement des cibles et niveaux d'alerte correspondants. Les SPI des SGS figurant dans les colonnes de droite des tableaux indiquent la corrélation nécessaire entre les indicateurs de sécurité du PNS et des SGS. Ces tableaux-résumés peuvent être compilés par l'État et remplis avec le plus grand nombre possible d'indicateurs de sécurité existants ou viables. Les SPI des SGS devront être établis par les fournisseurs de services par rapport avec les attentes des indicateurs de sécurité du PNS national. Afin d'assurer la concordance entre ces deux types d'indicateurs, l'État devra solliciter activement la participation des fournisseurs de services à l'établissement des SPI des SGS. Ces derniers seront probablement plus détaillés que les indicateurs de sécurité du PNS. À partir de cette banque d'indicateurs de sécurité, l'État peut alors sélectionner une série appropriée d'indicateurs pour la surveillance et la mesure de l'ALoSP de son PNS. Il est possible que certains indicateurs de sécurité/qualité soient maintenus (par l'État ou les fournisseurs de services) à des fins supplémentaires et n'ont donc pas à être retenus aux fins de surveillance et de mesure au niveau du PNS (ou SGS). Il s'agirait normalement d'indicateurs de bas niveau ou propres à certains processus de l'organisation.

2. Le Tableau 4-A4-5 (exemple de graphique d'indicateurs de sécurité de PNS) donne un exemple sous forme graphique d'indicateur de performance de sécurité à conséquences élevées. Dans le cas présent, il s'agit des taux d'incidents combinés de tous les exploitants dont le rapport est obligatoire. Le graphique de gauche montre les performances de l'année précédente, et celui de droite les tendances progressives prévues de l'année en cours. L'établissement du niveau d'alerte est fondé sur des critères d'écart standard de sécurité de base. La formule du chiffrier Excel est « =STDEVP ». Aux fins du calcul manuel de l'écart standard, la formule se présente comme suit :

$$\sigma = \sqrt{\frac{\sum (x - \mu)^2}{N}}$$

où « X » est la valeur de chaque point de données, « N » est le nombre de points de données et « μ » est la valeur moyenne de tous les points de données.

3. L'établissement de cible vise une amélioration de pourcentage (5 % dans ce cas) par rapport à la moyenne des points de données de l'année précédente. Il convient de noter que le dénominateur réel d'intervalle de points de données et celui du taux d'occurrence doivent être déterminés en fonction de la nature de chaque série de données, afin d'assurer la viabilité de l'indicateur de sécurité. Pour les événements à très faible fréquence, l'intervalle des points de données devra peut-être être établie sur une base annuelle plutôt que trimestrielle. De même, le dénominateur du taux d'occurrence peut être par 100 000 mouvements aériens, par exemple, au lieu de 1 000 mouvements. Le graphique illustré est fondé sur la fiche de données figurant dans le Tableau 4-A4-6.

4. La fiche de données du Tableau 4-A6 (fiche de données pour un échantillon de graphique d'indicateurs de sécurité) a servi à produire le graphique du Tableau 4-A4-5. Elle peut aussi être utilisée pour créer d'autres graphiques avec les données appropriées et la description adaptée des indicateurs de sécurité. Les trois lignes d'alerte et de cible sont créées automatiquement en fonction des paramètres respectifs indiqués dans la fiche de données.

5. Le Tableau 4-A4-7 (exemple d'un résumé des performances de l'ALoSP du PNS) résume tous les indicateurs de sécurité du PNS national, avec les résultats indiqués des cibles et des niveaux d'alerte respectifs. Un tel sommaire peut être compilé à la fin de chaque période de surveillance, pour donner une vue générale des performances de l'ALoSP du PNS. Si une mesure plus quantitative est souhaitable dans le résumé des performances, des points appropriés peuvent être affectés à chaque réponse Oui/Non pour chaque cible et niveau d'alerte. Exemples :

Indicateurs à conséquences élevées :

Niveau d'alerte non dépassé	[Oui (4), Non (0)]
Cible atteinte	[Oui (3), Non (0)]

Indicateurs à faibles conséquences :

Niveau d'alerte non dépassé	[Oui (2), Non (0)]
Cible atteinte	[Oui (1), Non (0)]

Ceci peut permettre d'obtenir un sommaire de note (ou pourcentage) indiquant la performance globale des indicateurs de sécurité de l'ALoSP à la fin de toute période de surveillance donnée.

Tableau 4-A4-1. Indicateurs de performance de sécurité pour les exploitants aériens

<i>Indicateurs de sécurité du PNS (globaux — État)</i>						<i>Indicateurs de performance de sécurité de SGS (individuels — fournisseur de services)</i>					
<i>Indicateurs à conséquences élevées (fondés sur les événements/résultats)</i>			<i>Indicateurs à faibles conséquences (fondés sur les événements/activités)</i>			<i>Indicateurs à conséquences élevées (fondés sur les événements/résultats)</i>			<i>Indicateurs à faibles conséquences (fondés sur les événements/activités)</i>		
<i>Indicateur de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de performance de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de performance de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>
Exploitants aériens (exploitants aériens de l'État seulement)											
Taux global d'accident/incident grave mensuel/trimestriel d'exploitants aériens de l'AAC (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	% LEI ou taux global annuel de conclusions des audits de surveillance des exploitants aériens de l'AAC (conclusions par audit)	Considération	Considération	Taux mensuel d'incidents graves des différentes flottes d'exploitants aériens (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	Taux mensuel d'incidents de l'ensemble des flottes des exploitants (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen
Taux trimestriel global d'IFSD de moteur des exploitants aériens de l'AAC (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	% LEI ou taux global annuel de conclusions des audits de surveillance des exploitants aériens de l'AAC (conclusions par audit)	Considération	Considération	Taux mensuel d'incidents graves de l'ensemble des flottes d'exploitants aériens (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	% LEI ou taux annuel de conclusions d'audits internes OMS/SGS d'exploitants (conclusions par audit)	Considération	Considération
			% LEI moyen annuel d'inspection de piste de surveillance de piste d'exploitants aériens étrangers de l'AAC (pour chaque exploitant étranger)	Considération	Considération	Taux d'incident d'IFSD de moteur d'exploitants aériens (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	Taux de rapports volontaires de dangers des exploitants (p. ex. par 1 000 FH)	Considération	Considération
			Taux global de rapports d'accident DGR d'exploitants de l'AAC (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen				Taux de rapports d'incidents DGR d'exploitants (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen
etc.											

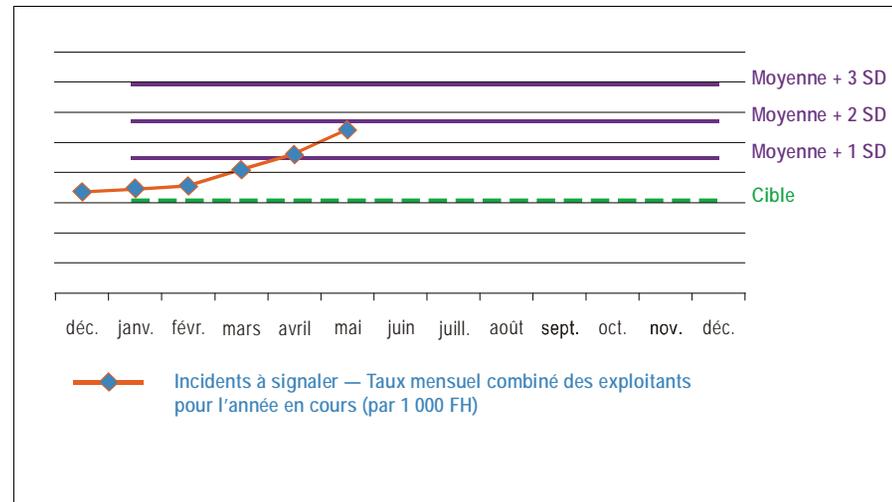
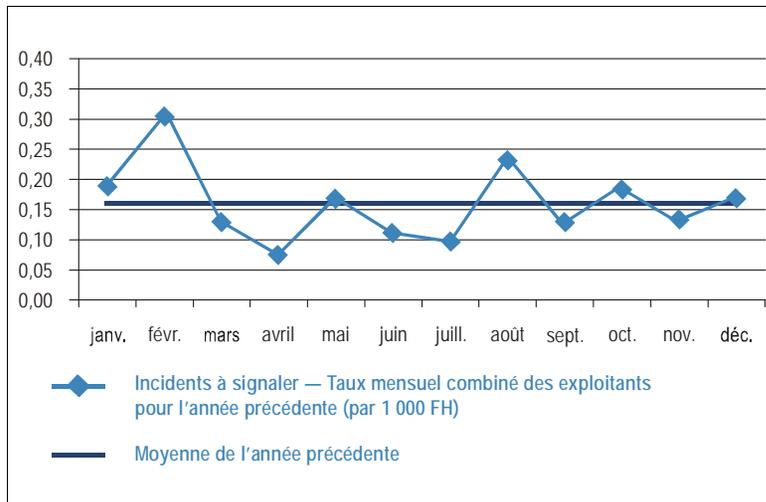
Tableau 4-A4-3. Indicateurs de performance de sécurité pour les exploitants ATS

<i>Indicateurs de performance de sécurité du PNS (globaux — État)</i>						<i>Indicateurs de performance de sécurité de SGS (individuels — fournisseur de services)</i>					
<i>Indicateurs à conséquences élevées (fondés sur les événements/résultats)</i>			<i>Indicateurs à faibles conséquences (fondés sur les événements/activités)</i>			<i>Indicateurs à conséquences élevées (fondés sur les événements/résultats)</i>			<i>Indicateurs à faibles conséquences (fondés sur les événements/activités)</i>		
<i>Indicateur de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de performance de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de performance de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>
Exploitants ATS											
Taux global trimestriel d'incidents graves dans les FIR (espace aérien) ATS de l'AAC — avec tous types d'aéronefs (p. ex. par 10 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	___ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	Taux global trimestriel d'incidents dans les FIR TCAS RA de l'AAC — avec tous types d'aéronefs (p. ex. par 10 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	___ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	Taux trimestriel d'incidents graves d'exploitants ATS dans les FIR — avec tous types d'aéronefs (p. ex. par 10 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	___ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	Taux trimestriel d'incidents d'exploitants ATS dans les FIR TCAS — avec tous types d'aéronefs (p. ex. par 10 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	___ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen
			Taux global trimestriel d'incident d'écart ATS au niveau des FIR (LOS) de l'AAC — avec tous types d'aéronefs (p. ex. par 10 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	___ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	Taux trimestriel/annuel de quasi-collisions d'exploitants ATS (p. ex. par 10 000 mouvements aériens)	En supposant que le taux moyen historique est 3, le taux d'alerte possible serait de 5.	En supposant que le taux moyen historique est 3, le taux d'alerte possible serait de 2.	Taux global trimestriel d'incident d'écart ATS au niveau des FIR (LOS) de l'AAC — avec tous types d'aéronefs (p. ex. par 10 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	___ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen
			% LEI ou taux globaux annuels des constatations des audits de surveillance des exploitants ATS de l'AAC (conclusions par audit)	Considération	Considération				% LEI annuel d'audit ou taux de constatations annuels QMS/SGS internes d'exploitants ATS (conclusions par audit)	Considération	Considération
etc.											

Tableau 4-A4-4. Organisations POA/DOA/MRO

<i>Indicateurs de performance de sécurité du PNS (globaux — État)</i>						<i>Indicateurs de performance de sécurité de SGS (individuels — fournisseur de services)</i>					
<i>Indicateurs à conséquences élevées (fondés sur les événements/résultats)</i>			<i>Indicateurs à faibles conséquences (fondés sur les événements/activités)</i>			<i>Indicateurs à conséquences élevées (fondés sur les événements/résultats)</i>			<i>Indicateurs à faibles conséquences (fondés sur les événements/activités)</i>		
<i>Indicateur de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de performance de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de performance de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>
Organisations DOA/POA/MRO											
Rapports globaux obligatoires de défauts MRO (MDR) reçus de l'AAC	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	% LEI ou taux globaux annuels de constatations d'audit de surveillance MRO/POA/DOA de l'AAC (conclusions par audit)	Considération	Considération	Taux trimestriel de réclamations de garantie technique	Moyenne + 1/2/3 SD (remise à 0 annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration entre chaque taux annuel moyen	% LEI ou taux annuel de constatations d'audits MRO/POA/DOA de QMS/SGS internes (conclusions par audit)	Considération	Considération
Taux global trimestriel POA/DOA de produits opérationnels qui font l'objet d'AD/ASB (par ligne de produit)	Considération	Considération				Taux trimestriel de produits opérationnels POA/DOA qui font l'objet d'AD/ASB (par ligne de produit)	Considération	Considération	Taux trimestriel MRO/POA/DOA d'inspection finale/de tests ratés/de rejet (dus à des problèmes internes de qualité)	Considération	Considération
						Taux trimestriel MRO/POA de rapports obligatoires sur des défaillances d'élément/défauts graves (en raison de problèmes internes de qualité)	Considération	Considération	Taux de rapports volontaires MRO/POA/DOA sur les risques (par employé opérationnel par trimestre)	Considération	Considération
etc.											

Tableau 4-A4-5. Exemple de graphique d'indicateurs de performance de sécurité de PNS (avec niveaux d'alerte et de cible)



a) Établissement de niveaux d'alerte :

Le niveau d'alerte d'une nouvelle période de surveillance (année en cours) est fondé sur les performances de la période précédente (année précédente), c'est-à-dire la moyenne des points de données et l'écart standard (SD). Les trois lignes de niveau d'alerte sont : moyenne + 1 SD, moyenne + 2 SD et moyenne + 3 SD.

b) Déclenchement du niveau d'alerte :

Une alerte (tendance anormale/non acceptable) est affichée si l'une quelconque des conditions ci-après est atteinte durant la période de surveillance en cours (année en cours) :

- tout point au-dessus de la ligne 3 SD
- 2 points consécutifs au-dessus de la ligne 2 SD
- 3 points consécutifs au-dessus de la ligne 1 SD.

Lorsqu'une alerte est déclenchée (risque potentiel élevé ou situation incontrôlable), des mesures de suivi appropriées sont attendues, par exemple une analyse pour déterminer la source et la cause-origine du taux d'incident anormal, ainsi que toute mesure requise pour redresser cette tendance non acceptable.

c) Établissement du niveau cible (amélioration planifiée) :

L'établissement du niveau cible peut être moins structuré que celui du niveau d'alerte, par exemple le taux moyen visé pour la nouvelle période de surveillance (année en cours) serait inférieur de, disons, 5 % (donc meilleur) par rapport la valeur moyenne de la période précédente.

d) Réalisation des cibles :

À la fin de l'année en cours, si le taux moyen de l'année en cours est inférieur de 5 % au moins ou davantage par rapport au taux moyen de l'année précédente, la cible établie de 5 % d'amélioration est considérée comme étant atteinte.

e) Niveaux d'alerte et de cible — période de validité :

Il convient de revoir/de rétablir les niveaux d'alerte et de cible pour chaque nouvelle période de surveillance, en fonction du taux moyen équivalent de la période précédente et de l'écart standard (SD), selon le cas.

Tableau 4-A4-6. Exemple de fiche de données utilisée pour créer un graphique d'indicateurs de sécurité à conséquences élevées de PNS (avec des critères d'établissement de niveaux d'alerte et de cible)

Année précédente				
Mois	Total FH de tous les exploitants	Incidents de tous les exploitants	Taux d'incident*	Moyenne
Janvier	51 837	10,00	0,19	0,16
Février	48 406	15,00	0,31	0,16
Mars	53 354	7,00	0,13	0,16
Avril	52 513	4,00	0,08	0,16
Mai	54 037	9,00	0,17	0,16
Juin	52 673	6,00	0,11	0,16
Juillet	54 086	5,00	0,09	0,16
Août	54 043	13,00	0,24	0,16
Septembre	52 383	7,00	0,13	0,16
Octobre	53 042	10,00	0,19	0,16
Novembre	51 353	7,00	0,14	0,16
Décembre	53 006	9,00	0,17	0,16
		Moyenne	0,16	
		SD	0,06	

Moyenne + 1 SD	Moyenne + 2 SD	Moyenne + 3 SD
0,23	0,29	0,35

Le critère d'établissement du niveau d'alerte de l'année en cours est fondé sur l'année précédente (Moyenne + 1/2/3 SD).

* Calcul du taux (par 1 000 FH).

Année en cours							
Mois	Total FH de tous les exploitants	Incidents de tous les exploitants	Taux d'incident*	Moyenne de l'année précédente + 1 SD	Moyenne de l'année précédente + 2 SD	Moyenne de l'année précédente + 3 SD	Moyenne de la cible de l'année en cours
Décembre	53 006	9,00	0,17				
Janvier	51 635	9,00	0,17	0,23	0,29	0,35	0,15
Février	44 295	8,00	0,18	0,23	0,29	0,35	0,15
Mars	48 323	10,00	0,21	0,23	0,29	0,35	0,15
Avril	47 176	11,00	0,23	0,23	0,29	0,35	0,15
Mai	47 469	13,00	0,27	0,23	0,29	0,35	0,15
Juin				0,23	0,29	0,35	0,15
Juillet				0,23	0,29	0,35	0,15
Août				0,23	0,29	0,35	0,15
Septembre				0,23	0,29	0,35	0,15
Octobre				0,23	0,29	0,35	0,15
Novembre				0,23	0,29	0,35	0,15
Décembre				0,23	0,29	0,35	0,15
		Moyenne					
		SD					

La cible de l'année courante est une amélioration de, disons, 5 % du taux moyen de l'année en cours par rapport au taux moyen de l'année précédente, qui est : 0,15

Tableau 4-A4-7. Exemple de sommaire de l'ALoSP du PNS de l'État « X » (disons pour l'année 2010)

<i>Indicateurs de sécurité à faibles conséquences</i>					
<i>Description du SI</i>		<i>Critères de niveau d'alerte du SI (pour 2010)</i>	<i>Niveau d'alerte franchi (Oui/Non)</i>	<i>Critères de niveau cible du SI (pour 2010)</i>	<i>Cible atteinte (Oui/Non)</i>
1	Taux global mensuel d'accident/incident grave d'exploitants aériens de l'AAC (par 1 000 FH)	Taux moyen de 2009 + 1/2/3 SD (rétabli chaque année)	Oui	Amélioration de <u>5 %</u> du taux moyen de 2010 par rapport au taux moyen de 2009	Non
2	Taux global mensuel d'accident/incident grave aux aérodromes de l'AAC — avec tous types d'aéronefs (par 10 000 mouvements au sol)	Taux moyen de 2009 + 1/2/3 SD (rétabli chaque année)	Oui	Amélioration de <u>3 %</u> du taux moyen de 2010 par rapport au taux moyen de 2009	Oui
3	Taux global mensuel d'incident grave de FIR de l'AAC — avec tous types d'aéronefs (par 10 000 mouvements au sol)	Taux moyen de 2009 + 1/2/3 SD (rétabli chaque année)	Non	Amélioration de <u>4 %</u> du taux moyen de 2010 par rapport au taux moyen de 2009	Non

<i>Indicateurs de sécurité à faibles conséquences</i>					
<i>Description du SI</i>		<i>Critères de niveau d'alerte du SI (pour 2010)</i>	<i>Niveau d'alerte franchi (Oui/Non)</i>	<i>Critères de niveau cible du SI (pour 2010)</i>	<i>Cible atteinte (Oui/Non)</i>
1	Résultats globaux d'audit/surveillance annuelle d'organisation d'exploitants aériens de l'AAC	LEI moyen de plus de 25 % ou toute conclusion de niveau 1, ou plus de 5 conclusions de niveau 2 par audit	Oui	LEI moyen de moins de 10 % et moins d'une conclusion de niveau 2 par audit	Non
2	% LEI moyen annuel d'inspection de surveillance d'escala d'exploitants aériens de l'AAC (pour chaque exploitant)	LEI moyen de plus de 25 % ou toute conclusion de niveau 1, ou plus de 5 conclusions de niveau 2 par audit	Oui	LEI moyen de moins de 10 %	Oui
3	Programme annuel d'inspection sur piste par échantillonnage d'exploitants étrangers de l'AAC	LEI moyen de plus de 25 % ou toute conclusion de niveau 1, ou plus de 5 conclusions de niveau 2 par audit, ou moins de 25 % d'exploitants étrangers inspectés	Oui	Pas moins de 50 % d'exploitants étrangers à inspecter	Non
4	Résultats globaux annuels d'audits/surveillance d'organisation d'exploitants d'aérodrome de l'AAC	LEI moyen de plus de 25 % ou toute conclusion de niveau 1, ou plus de 5 conclusions de niveau 2 par audit	Non	LEI moyen de moins de 10 % et moins d'une conclusion de niveau 2 par audit	Non

<i>Indicateurs de sécurité à faibles conséquences</i>					
<i>Description du SI</i>		<i>Critères de niveau d'alerte du SI (pour 2010)</i>	<i>Niveau d'alerte franchi (Oui/Non)</i>	<i>Critères de niveau cible du SI (pour 2010)</i>	<i>Cible atteinte (Oui/Non)</i>
1	Résultats globaux annuels d'audits/surveillance d'organisation d'exploitants ATS de l'AAC	LEI moyen de plus de 25 % ou toute conclusion de niveau 1, ou plus de 5 conclusions de niveau 2 par audit	Oui	LEI moyen de moins de 10 % et moins d'une conclusion de niveau 2 par audit	Oui
2	Taux global trimestriel de RA TCAS FIR ATS de l'AAC — avec tous types d'aéronefs (par 10 000 mouvements aériens)	Taux moyen de 2009 + 1/2/3 SD (rétabli chaque année)	Oui	Amélioration de 5 % du taux moyen de 2010 par rapport au taux moyen de 2009	Non
3	Résultats globaux annuels d'audits/surveillance D&M/MRO de l'AAC	LEI moyen de plus de 25 % ou toute conclusion de niveau 1, ou plus de 5 conclusions de niveau 2 par audit	Oui	LEI moyen de moins de 10 % et moins d'une conclusion de niveau 2 par audit	Oui
4	Taux global trimestriel de réclamations de garantie de pièces AMO (MRO) en raison de défauts techniques (majeures) de l'AAC	Taux moyen de 2009 + 1/2/3 SD (rétabli chaque année)	Non	Amélioration de 5 % du taux moyen de 2010 par rapport au taux moyen de 2009	Non

Note 1.— Autres indicateurs de procédures. Outre les indicateurs de sécurité au niveau du PNS ci-dessus, il peut y avoir d'autres indicateurs au niveau des systèmes dans chaque secteur d'exploitation. Exemples : indicateurs de procédures ou indicateurs de surveillance propres à des systèmes dans AIR, OPS ou AGA, ou des indicateurs liés à des programmes fondés sur les performances, tels que la gestion des risques de fatigue ou la gestion du carburant. De tels indicateurs de procédures ou propres à des systèmes devraient théoriquement être administrés dans le cadre du système ou de la procédure en question. Ils peuvent être considérés comme des indicateurs au niveau de systèmes particuliers ou de procédures qui forment la fondation des indicateurs de sécurité de surveillance de plus haut niveau du PNS. Il convient d'en tenir compte dans les manuels/SOP des systèmes ou des procédures respectifs, selon le cas. Néanmoins, les critères d'établissement des niveaux d'alerte ou de cible pour ces indicateurs devraient préférablement être conformes aux critères des indicateurs de sécurité au niveau du PNS, le cas échéant.

Note 2.— Sélection d'indicateurs et de niveaux. La combinaison (ou ensemble) d'indicateurs de sécurité à conséquences faibles ou élevées doit être sélectionnée par un État en fonction de l'ampleur de son système d'aviation. Dans le cas d'indicateurs où les critères suggérés d'établissement de niveaux d'alerte ou de cible ne sont pas applicables, l'État peut envisager tout autre critère de remplacement qu'il jugerait approprié. Il est conseillé en général d'établir des niveaux d'alerte ou de cible qui tiennent compte des performances historiques récentes ou actuelles.

Appendice 5 au Chapitre 4

PROTECTION DES INFORMATIONS DE SÉCURITÉ

1.1 Les dossiers remarquables de l'aviation civile internationale en matière de sécurité sont dus entre autres à un facteur essentiel : le processus d'apprentissage continu fondé sur l'établissement et le libre échange d'informations de sécurité. Il a été longtemps reconnu que les initiatives visant à renforcer la sécurité de l'aviation civile moderne doivent être fondées sur des données objectives. L'aviation civile dispose de plusieurs sources pour obtenir de telles données. Ensemble, elles constituent la base d'une compréhension rigoureuse des forces et des faiblesses des opérations aériennes.

1.2 Les informations tirées des enquêtes sur les accidents et incidents ont depuis toujours formé la clé de voûte des activités visant à améliorer la conception des équipements, les procédures de maintenance, la formation des équipages de conduite, les systèmes de contrôle de la circulation aérienne, l'aménagement et les fonctions des aéroports, les services météorologiques et d'autres aspects critiques de sécurité du système de transport aérien. Durant ces dernières années, la disponibilité de moyens technologiques a eu pour résultat l'éclosion rapide des systèmes de collecte et de traitement de données de sécurité (SDCPS).

1.3 Les SDCPS ont permis à la communauté de l'aviation civile d'acquiescer une compréhension approfondie des erreurs opérationnelles : le pourquoi de leur occurrence, ce qu'on peut faire pour minimiser leurs incidences et comment atténuer leur effet néfaste sur la sécurité. Il n'en reste pas moins que des situations dangereuses contribuent à des erreurs opérationnelles en aviation, dont la grande majorité sont involontaires. Des personnes bien formées, bien intentionnées commettent des erreurs lorsqu'elles assurent l'entretien, l'utilisation ou le contrôle d'équipement bien conçu. Dans les rares cas où des actes sont considérés, selon la loi, comme étant posés dans le but exprès de causer des dégâts, ou posés en connaissance de cause qu'il en résulterait des dégâts, ce qui est équivalent à une conduite imprudente, une négligence grave ou une faute intentionnelle, des systèmes d'exécution sont en place pour assurer que la chaîne de responsabilité reste intacte. Cette double approche, qui conjugue une meilleure compréhension des erreurs opérationnelles involontaires avec une application appropriée de la loi par les autorités compétentes le cas échéant, a bien servi l'aviation civile en termes de sécurité, tout en assurant que les auteurs d'infraction ne seront pas tolérés.

1.4 Or, une tendance s'est dégagée ces dernières années en aviation civile, selon laquelle, dans les cas où des erreurs opérationnelles ont été à l'origine d'incidents, les informations découlant des SDCPS ont été utilisées à des fins disciplinaires et d'application de la loi. Dans certains cas, elles ont même été admises comme preuves dans des procédures judiciaires, entraînant des accusations criminelles contre les personnes impliquées dans ces incidents. Les dépôts d'accusations criminelles dans les cas d'incidents d'aviation résultant d'erreurs opérationnelles non intentionnelles risquent de nuire à la soumission de rapports sur de tels événements, empêchant ainsi l'établissement et le libre échange d'informations de sécurité qui sont essentielles pour le renforcement de la sécurité de l'aviation.

1.5 Au sein de la communauté de l'aviation civile, un certain nombre d'initiatives ont été lancées pour essayer de protéger les SDCPS. Or, la question étant particulièrement délicate, il est essentiel de disposer d'un cadre qui apporterait la cohérence et un objectif commun de l'action de la communauté de l'aviation civile. Les efforts menés pour assurer la protection des informations de sécurité doivent réaliser un équilibre très délicat entre la nécessité de protéger les informations de sécurité, la nécessité du contrôle de la qualité, la nécessité de gérer les risques de sécurité et l'administration appropriée de la justice. Une démarche prudente s'impose donc à cet égard, pour éviter de formuler des propositions qui risquent d'aller à l'encontre de lois sur l'administration de la justice dans les États contractants.

1.6 Pour résoudre cette question, l'OACI a élaboré l'appendice E à l'Annexe 13, qui contient des orientations juridiques afin d'aider les États à promulguer des lois et des règlements nationaux destinés à protéger les informations tirées des SDCPS, tout en permettant l'exercice approprié de la justice. L'objectif visé est de prévenir l'usage indu d'informations recueillies dans le but exprès de renforcer la sécurité de l'aviation. Sachant que les États devraient pouvoir disposer de souplesse dans l'élaboration de leurs lois et règlements conformément à leurs politiques et pratiques nationales, ces orientations juridiques sont présentées sous forme d'une série de principes ci-après, qui peuvent être adaptés pour répondre aux besoins particuliers de l'État promulguant des lois et des règlements pour protéger les informations de sécurité.

1.7 Les orientations juridiques comprennent des principes généraux stipulant ce qui suit :

- a) le seul objet de la protection des informations de sécurité contre les usages indus est d'assurer qu'elles restent disponibles, afin de permettre l'adoption de mesures de prévention appropriées et opportunes et le renforcement de la sécurité de l'aviation ;
- b) la protection des informations de sécurité n'a pas pour objet de contrecarrer l'administration appropriée de la justice dans les États ;
- c) les lois et règlements nationaux protégeant les informations de sécurité devraient assurer un équilibre entre la nécessité de protéger les informations de sécurité pour renforcer la sécurité aérienne et la nécessité d'assurer l'administration appropriée de la justice ;
- d) les lois et règlements nationaux protégeant les informations de sécurité devraient en empêcher l'usage indu ;
- e) les responsabilités de sécurité d'un État incluent la protection des informations de sécurité appropriées dans des conditions spécifiées.

1.8 Les orientations comprennent des principes de protection comme suit :

- a) les informations de sécurité devraient bénéficier de la protection contre un usage indu selon des conditions spécifiées qui devraient inclure, sans s'y limiter, la collecte d'informations à des fins explicites de sécurité, dont la divulgation en éliminerait la disponibilité continue ;
- b) la protection devrait s'appliquer spécifiquement à chaque SDCPS, selon la nature des informations de sécurité qui y figurent ;
- c) il convient d'établir une procédure officielle pour assurer la protection des informations de sécurité appropriées, conformément aux conditions spécifiées ;
- d) les informations de sécurité ne devraient pas être utilisées pour des fins autres que celles pour lesquelles elles ont été recueillies ;
- e) les informations de sécurité ne devraient être utilisées dans des procédures disciplinaires, civiles, administratives et criminelles qu'avec des mesures de protection appropriées.

1.9 Il est recommandé que, dans les circonstances décrites ci-après, les informations de sécurité ne fassent pas l'objet de protection :

- a) il est prouvé que l'incident a été causé par un acte accompli, selon les dispositions de la loi, dans le but de causer des dommages ou avec la connaissance que des dommages en résulteraient probablement, ce qui équivaut à une conduite imprudente, une négligence grave ou une faute intentionnelle ;

- b) une autorité compétente considère que les circonstances semblent indiquer normalement que l'incident aurait pu être causé par une conduite avec l'intention de causer des dommages, ou une conduite menée avec la connaissance que des dommages en résulteraient probablement, ce qui équivaut à une conduite imprudente, une négligence grave ou une faute intentionnelle ; ou
- c) un examen entrepris par une autorité compétente détermine que la divulgation des informations de sécurité est nécessaire pour l'administration appropriée de la justice, et que leur révélation l'emporte sur l'effet néfaste qu'une telle divulgation aurait pu causer sur la disponibilité future des informations de sécurité à l'échelle nationale ou internationale.

1.10 Les orientations portent également sur la question de la divulgation publique et proposent que, sous réserve des principes de protection et avec les exceptions décrites ci-dessus, toute personne souhaitant la divulgation d'informations de sécurité devrait en justifier la révélation. Il convient d'établir des critères formels de divulgation des informations de sécurité qui incluraient les éléments ci-après, sans nécessairement s'y limiter :

- a) la divulgation d'informations de sécurité est nécessaire pour rectifier les conditions qui compromettent la sécurité et/ou pour modifier des politiques et des règlements ;
- b) la divulgation d'informations de sécurité ne portent pas atteinte à leur disponibilité future aux fins de renforcement de la sécurité ;
- c) la divulgation de renseignements personnels pertinents inclus dans les informations de sécurité est conforme aux lois applicables sur la vie privée ;
- d) la divulgation d'informations de sécurité se fait sous une forme sommaire ou globale, où les facteurs d'identification ont été éliminés.

1.11 Les orientations couvrent la responsabilité du dépositaire des informations de sécurité, et propose que chaque SDCPS désigne un dépositaire d'informations de sécurité, dont la responsabilité est d'appliquer toutes les protections possibles contre la divulgation des informations, sauf dans les circonstances suivantes :

- a) le dépositaire des informations de sécurité a le consentement de la source de l'information à ce que cette information soit divulguée ; ou
- b) le dépositaire des informations de sécurité est convaincu que la divulgation des informations de sécurité est conforme aux principes d'exception.

1.12 Enfin, les orientations introduisent la protection d'informations enregistrées et, sachant que l'enregistrement du fonds sonore ambiant du lieu de travail est exigé par la loi, dans le cas par exemple des enregistreurs de conversations de poste de pilotage (CVR), ce qui peut être perçu comme une invasion de la vie privée du personnel opérationnel, à laquelle les autres professions ne sont pas exposées, ces orientations proposent ce qui suit :

- a) sous réserve des principes de protection et d'exception ci-dessus, les lois et règlements nationaux devraient considérer les enregistrements du fonds sonore ambiant du lieu de travail exigés par la loi comme étant des informations confidentielles protégées, c'est-à-dire appelant une protection plus stricte ;
- b) les lois et règlements nationaux devraient contenir des mesures spécifiques de protection de ces enregistrements, en termes de leur confidentialité et de l'accès du public. Ces mesures particulières de protection des enregistrements requis par la loi peuvent inclure la promulgation d'ordonnances de non-divulgation au public.

1.13 Bien que les orientations sur la protection des SDCPS aient été adoptées le 3 mars 2006 comme une pièce jointe à l'Annexe 13, la communauté aéronautique a recommandé que l'OACI poursuive ses activités relatives à la protection des données et des informations de sécurité, afin d'en assurer la disponibilité aux fins de renforcement de la sécurité. En conséquence, à sa 37^e session, l'Assemblée a chargé le Conseil d'envisager de renforcer les dispositions sur la protection des informations de sécurité. Le 7 décembre 2010, la Commission de navigation aérienne a approuvé l'établissement de l'Équipe de travail sur la protection des informations de sécurité (SIP TF), qui a commencé ses travaux, le 5 mai 2011, sur les recommandations de dispositions et d'éléments d'orientation nouveaux ou améliorés portant sur la protection des informations de sécurité.

Appendice 6 au Chapitre 4

ORIENTATIONS SUR LA NOTIFICATION ET LE COMPTE RENDU D'ACCIDENTS ET D'INCIDENTS

1. INTRODUCTION

1.1 Conformément aux dispositions de l'Annexe 13 — *Enquêtes sur les accidents et incidents d'aviation*, les États sont tenus de communiquer à l'OACI des renseignements sur tous accidents d'aviation concernant des avions à turboréacteurs ayant une masse maximale certifiée au décollage supérieure à 2 250 kg. L'Organisation recueille également des renseignements sur les incidents d'aviation considérés comme importants pour la sécurité et la prévention d'accident. Aux fins de simplification, le mot « événement » (« occurrence » en anglais) désigne aussi bien un accident qu'un incident.

1.2 Dans les présentes orientations, les normes de l'Annexe 13 sont présentées dans un encadré gris.

2. ACCIDENTS ET INCIDENTS — NOTIFICATION ET RAPPORTS

2.1 Généralités

2.1.1 Le système OACI de comptes rendus d'accident et d'incident (ADREP) recueille des données des États afin de renforcer la sécurité par des analyses, fondées soit sur la validation de problèmes connus de sécurité, soit sur la détermination de tendances émergentes de sécurité, permettant d'élaborer des recommandations pour la prévention des accidents.

2.1.2 À la suite d'un événement, les informations pertinentes sont communiquées à l'OACI en quatre étapes différentes :

- a) notification ;
- b) rapport préliminaire (ADREP) ;
- c) rapport final ;
- d) rapport de données (ADREP).

Les quatre étapes sont examinées en détail dans les Sections 2.2 à 2.5 ; le Tableau 4-A6-1 est un résumé séquentiel d'une liste de vérification de la notification et du compte rendu, conformément à l'Appendice B à l'Annexe 13.

2.1.3 Pour faciliter la soumission des comptes rendus, les États peuvent désormais utiliser le portail protégé de l'OACI en ligne pour soumettre des notifications et des rapports ADREP par formulaire électronique ou sous un format compatible au système ADREP (p. ex. ECCAIRS). La Section 3 contient d'autres directives sur les formulaires électroniques de l'OACI.

2.2 Notification

Une notification permet de diffuser immédiatement des informations sur un accident/incident. Conformément au Chapitre 4 de l'Annexe 13, les renseignements ci-après doivent être communiqués à l'OACI :

4.1 L'État d'occurrence adressera une notification d'accident ou d'incident grave dans les délais les plus brefs et par la meilleure et la plus rapide des voies disponibles :

- a) à l'État d'immatriculation ;
- b) à l'État de l'exploitant ;
- c) à l'État de conception ;
- d) à l'État de construction ;
- e) à l'Organisation de l'aviation civile internationale, quand la masse maximale de l'aéronef concerné est supérieure à 2 250 kg ou quand il s'agit d'un avion à turboréacteur.

Toutefois, lorsque l'État d'occurrence n'est pas au courant d'un incident grave, il appartiendra à l'État d'immatriculation ou à l'État de l'exploitant, selon le cas, de notifier cet incident à l'État de conception, à l'État de construction et à l'État d'occurrence.

...

4.2 La notification sera rédigée en langage clair et comprendra tous ceux des renseignements ci-après qui pourront être immédiatement obtenus, mais l'envoi de la notification ne devra pas être retardé du fait que ces renseignements seraient incomplets :

- a) abréviation d'identification ACCID, pour un accident, et INCID, pour un incident grave ;
- b) constructeur, modèle, marques de nationalité et d'immatriculation et numéro de série de l'aéronef ;
- c) nom du propriétaire et, le cas échéant, nom de l'exploitant et de l'affréteur de l'aéronef ;
- d) qualification du pilote commandant de bord et nationalité de l'équipage et des passagers ;
- e) date et heure (heure locale ou UTC) de l'accident ou de l'incident grave ;
- f) dernier point de départ de l'aéronef et point d'atterrissage prévu ;
- g) position de l'aéronef par rapport à un point de repère géographique facile à identifier, latitude et longitude ;
- h) nombre de membres d'équipage et de passagers ; à bord : tués et grièvement blessés ; autres : tués et grièvement blessés ;
- i) description de l'accident ou de l'incident grave et étendue des dommages causés à l'aéronef, dans la mesure où elle est connue ;
- j) indication de la mesure dans laquelle l'État d'occurrence mènera l'enquête ou se propose de déléguer ses pouvoirs pour la conduite de cette enquête ;

- k) caractéristiques physiques de la zone de l'accident ou de l'incident grave et indication des difficultés d'accès ou des dispositions spéciales concernant l'accès au site ;
- l) identification du service émetteur et moyen de contacter l'enquêteur désigné et le service d'enquête sur les accidents de l'État d'occurrence ;
- m) présence et description des marchandises dangereuses se trouvant à bord de l'aéronef.

2.3 Rapport préliminaire

2.3.1 Le rapport préliminaire est le mode de communication utilisé pour diffuser rapidement les données recueillies durant les premières phases de l'enquête. Il s'agit d'un rapport *ad interim* qui contient des renseignements supplémentaires qui manquaient ou n'étaient pas disponibles au moment de l'envoi de la notification. Les rapports préliminaires ne sont pas obligatoires pour les incidents. On trouvera la liste des renseignements à envoyer dans un rapport préliminaire à la page <http://www.icao.int/Safety/reporting>.

2.3.2 Les paragraphes 7.1 et 7.2 du Chapitre 7 de l'Annexe 13 stipulent ceci :

Accidents survenus à des aéronefs de plus de 2 250 kg

7.1 Lorsque l'aéronef accidenté est un aéronef d'une masse maximale supérieure à 2 250 kg, l'État qui mène l'enquête enverra le compte rendu préliminaire :

- a) à l'État d'immatriculation ou à l'État d'occurrence, selon le cas ;
- b) à l'État de l'exploitant ;
- c) à l'État de conception ;
- d) à l'État de construction ;
- e) à tout État qui aura fourni des renseignements pertinents, des moyens importants ou des experts ;
- f) à l'Organisation de l'aviation civile internationale.

Accidents survenus à des aéronefs de 2 250 kg ou moins

7.2 Lorsqu'un aéronef non visé par le § 7.1 est accidenté et que se posent des questions de navigabilité ou des questions qui peuvent présenter de l'intérêt pour d'autres États, l'État qui mène l'enquête enverra le compte rendu préliminaire :

- a) à l'État d'immatriculation ou à l'État d'occurrence, selon le cas ;
- b) à l'État de l'exploitant ;
- c) à l'État de conception ;

- d) à l'État de construction ;
- e) à tout État qui aura fourni des renseignements pertinents, des moyens importants ou des experts.

2.3.3 La paragraphe 7.4 du Chapitre 7 de l'Annexe 13 stipule ce qui suit :

Envoi

7.4 Le compte rendu préliminaire sera envoyé par télécopieur, courrier électronique ou poste aérienne dans les 30 jours qui suivent la date de l'accident, à moins que le compte rendu de données d'accident/incident n'ait été envoyé avant cette date. Lorsque se posent des questions intéressant directement la sécurité, ce compte rendu sera envoyé dès que les renseignements auront été obtenus et par la meilleure et la plus rapide des voies disponibles.

2.4 Rapport final

2.4.1 Les paragraphes 6.5 à 6.7 du Chapitre 6 de l'Annexe 13 contiennent les normes ci-après, relatives au rapport final :

Diffusion du rapport final

6.5 Pour contribuer à la prévention des accidents, l'État qui mène l'enquête sur un accident ou un incident rendra public le rapport final dans les plus brefs délais et, si possible, dans les 12 mois.

...

6.6 Si le rapport ne peut être rendu public dans les 12 mois, l'État qui a mené l'enquête émettra une déclaration intérimaire publique à chaque date anniversaire de l'occurrence, détaillant les progrès de l'enquête et toutes questions de sécurité qui auront été soulevées.

6.7 Lorsque l'État qui a mené l'enquête sur un accident ou un incident survenu à un aéronef d'une masse maximale supérieure à 5 700 kg a rendu public un rapport final, il en adressera un exemplaire à l'Organisation de l'aviation civile internationale.

2.4.2 Le *Manuel d'enquêtes sur les accidents et incidents d'aviation* (Doc 9756), Partie IV — *Communication des résultats*, contient des directives détaillées sur la forme de présentation, le contenu et la soumission du rapport final.

2.5 Rapport de données

2.5.1 Une fois l'enquête terminée et le rapport final approuvé, un rapport de données d'accident ou d'incident doit être compilé. Si une enquête est rouverte, les renseignements communiqués précédemment doivent être modifiés selon qu'il convient. L'objet du rapport de données est de fournir des informations exactes et complètes sous une forme standard.

2.5.2 On trouvera à la page <http://www.icao.int/Safety/reporting> les renseignements requis pour remplir un rapport de données.

2.5.3 Le paragraphe 7.5 du Chapitre 7 de l'Annexe 13 dispose par ailleurs :

Accidents survenus à des aéronefs de plus de 2 250 kg

7.5 Si l'aéronef accidenté a une masse maximale supérieure à 2 250 kg, l'État qui mène l'enquête enverra, aussitôt que possible après l'enquête, le compte rendu de données d'accident à l'Organisation de l'aviation civile internationale.

3. INSTRUCTIONS GÉNÉRALES POUR LA COMPILATION

3.1 Options pour le compte rendu d'événements à l'OACI

Les événements peuvent être signalés à l'OACI au moyen de l'une des options suivantes :

- a) Gestionnaire de rapport d'événement de l'OACI, disponible sur le portail protégé iSTARS à la page <http://www.icao.int/Safety> ;
- b) rapport de base de données compatible au système ADREP (p. ex. ECCAIRS) ;
- c) rapports imprimés envoyés à l'OACI.

3.2 Gestionnaire de rapport d'événement

Il est désormais possible de remplir électroniquement les formulaires de notification et de rapport préliminaire ADREP au moyen du gestionnaire de rapport d'événement de l'OACI, disponible sur le portail protégé d'iSTARS. Les membres d'iSTARS peuvent accéder aux formulaires de rapport d'événement en cliquant sur le lien contenant les instructions de compte rendu. Pour s'inscrire et accéder au portail protégé d'iSTARS, on peut en demander l'accès sur son site en ligne ou par courrier électronique à adrep@icao.int.

3.3 Règles de base

La validité des informations de sécurité que l'OACI fournit aux États dépend des détails et du soin avec lequel les événements ont été signalés. Il est donc dans l'intérêt de tous les États de communiquer des données exactes et complètes, conformément à l'Annexe 13 et aux orientations du présent manuel. Voici quelques règles de base à suivre pour remplir le formulaire de rapport d'accident et d'incident en ligne de l'OACI ou le format compatible avec le système ADREP (p. ex. ECCAIRS) :

- a) Déterminer la classification et la catégorie appropriées de l'événement, c'est-à-dire, s'agit-il d'un accident, d'un incident grave ou d'un incident, selon le degré de blessures, de dégâts à l'aéronef et autres renseignements disponibles.
- b) Inscrire les données essentielles : date, heure, État et lieu de l'événement, aéroport, gravité, type d'aéronef, exploitant, type d'opération et phase de vol.
- c) Choisir les unités de champs appropriées avant d'inscrire les valeurs, par exemple ft, MSL ou FL pour l'altitude.

- d) Si plus d'un aéronef est impliqué dans un événement, fournir les renseignements sur l'autre aéronef. Pour remplir la case sur le type d'événement dans le cas de plusieurs aéronefs, s'assurer de bien distinguer les aéronefs (1 ou 2). Tous les événements doivent être décrits dans un ordre séquentiel ; s'assurer de ne pas omettre des éléments vitaux.
- e) Aligner les événements sur les catégories d'événement.
- f) N'utiliser l'inscription « Inconnu » que s'il est établi après enquête que le renseignement visé n'a pas été trouvé.
- g) Utiliser l'inscription « Blanc » pour indiquer que l'enquête est en cours afin de trouver le renseignement qui n'est actuellement pas disponible.

3.4 Notifications

3.4.1 Pour remplir une notification au moyen du gestionnaire de rapport d'événement d'iSTARS, tous les renseignements requis conformément au paragraphe 4.2 du Chapitre 4 de l'Annexe 13 sont contenus dans les formulaires de notification électroniques qui sont disponibles en ligne et qui doivent être remplis selon les instructions y figurant.

3.4.2 Certains champs du formulaire de notification sont des identificateurs clés qui aideront l'OACI à identifier les rapports dans la base de données. Ainsi, dans le cas de soumission électronique, ces champs doivent être remplis pour la soumission de la notification initiale :

- a) État de compte rendu ;
- b) Numéro de dossier de l'État ;
- c) Organisation de compte rendu ;
- d) Classe d'événement ;
- e) Date de l'événement.

3.4.3 Durant l'inscription de données de base, telles que le degré de blessure et de dégât à l'aéronef, il faut s'assurer d'aligner ces sélections sur la classe de l'événement. Par exemple, si l'événement a été classé comme un accident, le degré de blessure doit être grave, fatal ou inconnu, tandis que l'état de l'aéronef doit être « dégâts substantiels », « détruit » ou « inconnu ».

3.5 Taxonomie ADREP

La taxonomie ADREP, conçue par l'OACI, contient des définitions et une terminologie pour les systèmes de compte rendu d'accident et incident d'aviation. Les documents de taxonomie peuvent être consultés à la page <http://www.icao.int/Safety/reporting>, chaque fois qu'il y a un doute de terminologie dans les notifications et les rapports.

3.6 Envoi des rapports

3.6.1 Si les informations sur l'événement sont disponibles dans un format compatible au système ADREP (p. ex. ECCAIRS), une copie du fichier électronique (p. ex. E4F) sera jointe à la notification électronique et envoyée à adrep@icao.int.

3.6.2 Les formulaires de rapport en ligne soumis électroniquement par le portail protégé d'iSTARS sont reçus directement par l'OACI. Les rapports sur papier imprimé doivent être envoyés à l'OACI à adrep@icao.int ou à l'adresse suivante :

Organisation de l'aviation civile internationale
999, rue University
Montréal, Québec H3C 5H7
Canada
Fax : + 1 514-954-6077

3.6.3 La notification et les rapports doivent être rédigés en langage simple et, si cela ne cause pas de retard indu, dans une des langues de travail de l'OACI, en tenant compte de la langue ou des langues des destinataires.

4. INSTRUCTIONS SPÉCIALES POUR LA COMPILATION

4.1 Codage de la catégorie de l'événement

4.1.1 La taxonomie ADREP des catégories d'événements fait partie du système de comptes rendus d'accident et d'incident de l'OACI. Ces catégories sont désignées par une série de termes utilisés par l'OACI pour classer les accidents et les incidents afin d'analyser les tendances en matière de sécurité. Ces analyses ont pour objet de permettre l'application de mesures préemptives visant à prévenir des accidents ou incidents similaires à l'avenir.

4.1.2 La séquence de la plupart des accidents et incidents comprend des événements multiples. Le codage strict d'un accident ou d'un incident dans une catégorie unique peut donc être difficile. Par exemple une manœuvre brusque (AMAN) peut entraîner en plus une perte de contrôle en vol (LOC-I). Dans un tel cas, l'événement est classé sous les deux catégories AMAN et LOC-I. La philosophie de l'OACI en matière de codage des catégories permet de coder un accident ou incident unique sous de multiples catégories, pour permettre à l'OACI d'envisager ou d'étudier tous les événements menant à l'accident ou l'incident. On trouvera des définitions détaillées des catégories d'événement et des instructions pour le codage de catégories multiples à <http://www.icao.int/Safety/reporting>.

4.2 Codage du type d'événement

4.2.1 Afin de déterminer les causes d'un accident ou d'un incident, il est essentiel d'étudier les facteurs précédant, durant ou suivant l'événement. C'est pourquoi il est vital que toutes les données connues au moment de la rédaction du rapport soient incluses avec exactitude.

4.2.2 Pour mieux décrire un événement, des « facteurs descriptifs » peuvent être inscrits pour chaque événement. Ces facteurs descriptifs décrivent en détails ce qui est arrivé durant l'événement en indiquant tous les phénomènes constatés. Si possible, les facteurs descriptifs devraient être codés dans l'ordre chronologique en dessous de chaque type d'événement.

4.2.3 Pour expliquer un événement, des « facteurs explicatifs » peuvent être inscrits pour chaque facteur descriptif. Ces facteurs expliquent pourquoi l'événement est survenu et incluent les aspects de facteurs humains dans le codage des événements. Ils permettent de déterminer les mesures préventives qui pourraient être requises. La série complète des types d'événement et la description détaillée des facteurs descriptifs et explicatifs sont présentées sur la page web de taxonomie ADREP de l'OACI.

4.2.4 Voici quelques considérations générales dont il faut tenir compte dans le compte rendu des événements :

- a) *Soyez aussi précis que possible, sans spéculer sur les détails.* Par exemple, si le train avant n'est pas sorti, utilisez la description « événement lié au train d'atterrissage avant/arrière » et non pas « événement lié au train d'atterrissage ».
- b) *Alignez les catégories d'événement avec les événements.* Par exemple, si la catégorie de l'événement est SCF-NP, il faut donc qu'il y ait eu une défaillance d'un élément/système non lié au groupe motopropulseur.
- c) *Alignez les événements et les facteurs descriptifs.* Les événements et les facteurs descriptifs décrivent ce qui a mal fonctionné, ce qui n'a pas fonctionné, ce qui est sorti de l'ordinaire et ce qui a contribué à l'événement. Par exemple, la description « événement lié à une alarme centrale » peut être utilisée pour des événements où le système a subi une défaillance, et le facteur descriptif « ordinateurs centraux » peut servir à préciser l'événement.
- d) *Inscrire la séquence des événements dans l'ordre chronologique.* Un événement doit être décrit par la façon dont il est codé. Essentiellement, le codage de l'événement doit donner une image de la séquence de l'événement similaire à celle qui figure dans l'exposé des faits.

4.3 Exposé des faits

4.3.1 L'exposé des faits donne une brève description de l'événement, notamment les circonstances de l'urgence, les faits significatifs et autres renseignements pertinents. L'exposé ne dépassera pas 200 mots. Il importe que les événements soient décrits dans l'ordre chronologique, de façon concise et spécifique.

4.3.2 L'étude et l'analyse de la séquence des événements qui ont mené à l'événement peuvent aider à mieux comprendre la nature de l'événement. C'est pourquoi les exposés des faits devraient inclure un résumé concis de tous les événements afin d'éclairer les événements qui ont donné lieu à l'incident. Il n'y a pas lieu de répéter dans le rapport de données les renseignements fournis dans l'exposé du rapport préliminaire. Par contre, toute nouvelle information obtenue après la soumission du rapport préliminaire doit être incluse dans le rapport de données. Considérés ensemble, les deux exposés des faits devraient brosser un tableau complet du vol et des conclusions de l'enquête.

4.3.3 Si un rapport préliminaire n'a pas été soumis (soit dans le cas d'un incident ou lorsqu'une enquête sur un accident n'est pas achevée dans les 30 jours), l'exposé des faits dans le rapport de données doit indiquer l'historique du vol et la description et l'analyse du comment et du pourquoi de l'événement, les conclusions de l'enquête, les constatations et les causes probables. Dans ces cas, le rapport de données soumis peut idéalement comprendre 400 mots au total.

4.4 Recommandations de sécurité

L'auteur du rapport doit mettre en corrélation les recommandations ou les mesures de sécurité avec les constatations pertinentes, le cas échéant. Les champs placés sous la recommandation de sécurité dans le rapport de données devraient inclure toute mesure correctrice prise ou envisagée. La recommandation devrait indiquer, si possible, comment la mesure correctrice résoudra le problème de sécurité détecté. Inclure un résumé de toute mesure préventive déjà prise.

Tableau 4-A6-1. Liste de vérification de notification et de compte rendu

Dans cette liste de vérification, les termes ci-après ont la signification indiquée ci-dessous :

Événements internationaux. Accidents et incidents graves survenus dans le territoire d'un État contractant à un aéronef immatriculé dans un autre État contractant.

Événements intérieurs. Accidents et incidents graves survenus dans le territoire de l'État d'immatriculation.

Autres événements. Accidents et incidents graves survenus dans le territoire d'un État non contractant, ou à l'extérieur du territoire d'un État quelconque.

Notification d'accidents et d'incidents graves

<i>De</i>	<i>Rapport</i>	<i>À</i>	<i>Pour</i>	<i>Délais</i>
État d'occurrence	Notification	État d'immatriculation État de l'exploitant État de conception État de fabrication	Événements internationaux : Tous les aéronefs	Avec un minimum de retard
		OACI	Aéronef de plus de 2 250 kg ou avions à turbopropulseurs	
État d'immatriculation	Notification	État de l'exploitant État de conception État de fabrication	Événements intérieurs et autres événements	
		OACI	Aéronef de plus de 2 250 kg ou avions à turbopropulseurs	

Rapport préliminaire ADREP

<i>De</i>	<i>Catégorie</i>	<i>Rapport</i>	<i>À</i>	<i>Pour</i>	<i>Délai</i>
État menant l'enquête	Accident	Préliminaire	État d'immatriculation État d'occurrence État de l'exploitant État de fabrication État de conception Tout État fournissant des informations, des moyens importants ou des experts OACI	Aéronefs de plus de 2 250 kg	30 jours*
			Idem, sauf pour l'OACI	Accidents survenus aux aéronefs de masse égale ou inférieure à 2 250 kg s'il y a des problèmes de navigabilité ou des questions d'intérêt	
	Incident	Préliminaire	Non requis		

*Si le rapport de données d'accident a été établi et envoyé à l'OACI dans un délai de 30 jours, aucun rapport préliminaire n'est requis.

Rapport final — Accident et incidents indépendamment du lieu d'occurrence

<i>De</i>	<i>Rapport</i>	<i>À</i>	<i>Pour</i>	<i>Délai</i>
État menant l'enquête	Rapport final	État lançant l'enquête État d'immatriculation État de l'exploitant État de conception État de fabrication État intéressé en raison des décès États fournissant des informations, des moyens importants ou des experts	Tous les aéronefs	Avec un minimum de retard
		OACI	Aéronefs de plus de 5 700 kg	

Rapport de données ADREP

<i>De</i>	<i>Catégorie</i>	<i>Rapport</i>	<i>À</i>	<i>Pour</i>	<i>Délai</i>
État menant l'enquête	Accident	Données	OACI	Aéronefs de plus de 2 250 kg	Une fois l'enquête terminée
État menant l'enquête	Incident	Données	OACI	Aéronefs de plus de 5 700 kg	Une fois l'enquête terminée

Appendice 7 au Chapitre 4

LISTE DE VÉRIFICATION DE L'ANALYSE DE L'ÉCART DU PNS ET PLAN DE MISE EN ŒUVRE

1. LISTE DE VÉRIFICATION DE L'ANALYSE INITIALE DE L'ÉCART (TABLEAU 4-A7-1)

1.1 La liste de vérification de l'analyse initiale de l'écart du Tableau 4-A7-1 peut servir de modèle pour réaliser la première étape d'une analyse de l'écart du PNS. Cette forme de présentation, avec ses réponses générales « Oui/Non/En partie » donnera une première indication de la vaste portée des écarts et donc un tableau général de la charge de travail à prévoir. Ces premiers renseignements devraient être utiles pour les cadres supérieurs pour anticiper l'étendue des efforts de mise en œuvre du PNS et donc des ressources à fournir. Cette liste de vérification initiale devra être suivie d'un plan approprié de mise en œuvre, comme l'indiquent les Tableaux 4-A7-2 et 4-A7-3.

1.2 Une réponse positive (« Oui ») indique que l'État répond aux attentes de la question ou les dépasse. Une réponse négative (« Non ») indique un écart substantiel dans le système en place par rapport aux attentes de la question. Une réponse partielle (« En partie ») indique que des travaux supplémentaires de renforcement ou d'amélioration d'un processus existant sont nécessaires pour répondre aux attentes de la question.

Note.— Les références SMM entre crochets [] indiquent les éléments d'orientation du présent manuel qui sont pertinents à la question de l'analyse de l'écart.

Tableau 4-A7-1. Liste de vérification de l'analyse de l'écart

N ^o	Aspect à analyser ou question à répondre	Réponse	État de mise en œuvre
Composant 1 — POLITIQUES ET OBJECTIFS NATIONAUX DE SÉCURITÉ			
Élément 1.1 — Cadre législatif national de la sécurité			
1.1-1	[État] a-t-il promulgué un cadre législatif national de la sécurité et des règlements spécifiques qui définissent la gestion de la sécurité dans l'État ? [4.2.1, Élément 1.1 ; 4.3.2 ; 4.4.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.1-2	Le cadre législatif et les règlements spécifiques sont-ils revus périodiquement pour assurer qu'ils restent pertinents pour l'État ? [4.2.1, Élément 1.1 ; 4.4.4 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 1.2 — Responsabilités et imputabilités de l'État en matière de sécurité			
1.2-1	[État] a-t-il identifié une organisation-signet du PNS et un cadre responsable de l'exécution et de la coordination du PNS ? [4.2.1, Élément 1.2 ; 4.4.3 a)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question à répondre	Réponse	État de mise en œuvre
1.2-2	[État] a-t-il établi une équipe de mise en œuvre du PNS ? [4.2.1, Élément 1.2 ; 4.4.3 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-3	[État] a-t-il défini ses besoins, ses responsabilités et ses imputabilités concernant l'établissement et le maintien du PNS ? [4.2.1, Élément 1.2 ; 4.4.3]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-4	[État] a-t-il mis en place un plan de mise en œuvre du PNS, qui inclut un calendrier pour l'exécution des mesures correctrices des écarts identifiés par l'analyse ? [4.3 ; 4.4.3 d)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-5	Y a-t-il un énoncé documenté sur la fourniture des ressources nécessaires à la mise en œuvre et au maintien du PNS ? [4.2.1, Élément 1.2 ; Chapitre 4, Appendice 1, Partie 1, 1.1 d)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-6	L'administrateur de l'[État] responsable du PNS a-t-il le contrôle des ressources nécessaires à la mise en œuvre du PNS ? [4.4.3 a)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-7	[État] a-t-il défini les activités et les imputabilités spécifiques à la gestion de la sécurité dans l'État dont chaque organisation de réglementation de l'aviation dans le PNS a la responsabilité ? [4.4.5 a)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-8	[État] a-t-il un mécanisme ou une plate-forme pour la coordination de la mise en œuvre du PNS et les activités ultérieures de surveillance continue auxquelles participent toutes les organisations de réglementation de l'État ? [4.4.3 e)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-9	L'administrateur de l'[État] responsable du PNS coordonne-t-il les activités des différentes organisations aéronautiques de l'État au titre du PNS ? [4.2.1, Élément 1.2 ; 4.4.3 a)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-10	[État] a-t-il établi une politique de la sécurité ? [4.2.1, Élément 1.2 ; 4.4.5 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-11	La politique de sécurité de l'[État] est-elle signée par l'administrateur de l'[État] responsable du PNS ou par une autorité compétente dans l'[État] ? [Chapitre 4, Appendice 1]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-12	La politique de sécurité de l'[État] est-elle revue périodiquement ? [4.4.15]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question à répondre	Réponse	État de mise en œuvre
1.2-13	La politique de sécurité de l'État est-elle communiquée aux employés de toutes les organisations aéronautiques de l'État afin de leur faire prendre conscience de leurs responsabilités individuelles en matière de sécurité ? [4.4.5 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-14	État a-t-il élaboré, dans le cadre du plan de mise en œuvre du PNS, un document unifié du PNS pour en décrire les composants et éléments du cadre ? [4.2.1, Élément 1.2 ; 4.4.3 f) ; Appendice 8]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-15	Le document du PNS est-il terminé, approuvé et signé par l'administrateur responsable du PNS et communiqué ou mis à la disposition de toutes les parties prenantes dès la mise en œuvre complète du PNS ? [4.4.3 f)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-16	État dispose-t-il d'un système de documentation permettant l'entreposage, l'archivage, la protection et la récupération appropriés de tous les documents liés aux activités du PNS ? [4.2.1, Élément 1.2 ; 4.4.3 f)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-17	État dispose-t-il d'un mécanisme de revue périodique interne permettant d'améliorer en permanence la qualité et l'efficacité du PNS ? [4.2.1, Élément 3.1 ; 4.4.15]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 1.3 — Enquête sur les accidents et incidents			
1.3-1	État a-t-il établi une procédure d'enquête indépendante d'accident et d'incident dont le seul objectif est de prévenir les accidents et les incidents et non pas de répartir les blâmes et les responsabilités ? [4.2.1, Élément 1.3 ; 4.4.6]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.3-2	L'organisation/autorité d'enquête sur les accidents est-elle fonctionnellement indépendante (voir le <i>Manuel d'enquête sur les accidents et incidents d'aviation</i> (Doc 9756, Partie I, 2.1) ? [4.4.6 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 1.4 — Politique d'application de la loi			
1.4-1	État a-t-il promulgué une politique d'application de la loi ? [4.2.1, Élément 1.4 ; 4.4.10 ; Appendices 10 et 11]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.4-2	La législation aéronautique principale de l'État prévoit-elle l'application des lois et règlements applicables ? [4.4.7]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question à répondre	Réponse	État de mise en œuvre
1.4-3	La politique d'application tient-elle compte du fait que les fournisseurs de services sont normalement autorisés à traiter et à résoudre de façon systématique les écarts de sécurité ou de qualité dans les limites de leurs procédures SGS/QMS approuvées ? [4.4.10 a)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.4-4	La politique d'application établit-elle les conditions et les circonstances dans lesquelles l'État peut régler directement les écarts de sécurité par ses procédures établies d'enquête et d'exécution ? [4.2.1, Élément 1.4 ; 4.4.10 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.4-5	La politique d'application du PNS comprend-elle des dispositions pour prévenir l'usage ou la divulgation de données de sécurité à des fins autres que le renforcement de la sécurité ? [4.2.1, Élément 1.4 ; 4.4.10 c)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.4-6	La politique d'application du PNS comprend-elle des dispositions pour protéger les sources des informations obtenues des systèmes de compte rendu volontaire d'incident ? [4.4.10 d) ; Appendices 2 et 10]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Composant 2 — GESTION DES RISQUES DE SÉCURITÉ PAR L'ÉTAT			
Élément 2.1 — Exigences de sécurité pour les SGS des fournisseurs de services			
2.1-1	[État] a-t-il promulgué des règlements harmonisés exigeant des fournisseurs de services qu'ils mettent en œuvre un SGS ? [4.2.1, Élément 2.1 ; 4.4.9 ; Appendice 9]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.1-2	Les dispositions et les éléments d'orientation connexes des SGS font-ils l'objet d'une révision périodique pour assurer qu'ils restent pertinents et appropriés pour les fournisseurs de services ? [4.2.1, Élément 2.1 ; 4.4.14 a)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 2.2 — Accord sur les performances de sécurité des fournisseurs de services			
2.2-1	L'[État] a-t-il approuvé/accepté individuellement les performances des indicateurs de sécurité des fournisseurs de services et leurs niveaux d'alerte/cible respectifs ? [4.2.1, Élément 2.2 ; 4.4.13]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.2-2	Les indicateurs de performance de sécurité acceptés/convenus sont-ils proportionnés à l'ampleur/complexité du contexte opérationnel particulier des différents fournisseurs de services ? [4.4.13]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.2-3	Les indicateurs de performance de sécurité convenus sont-ils revus périodiquement par l'[État] pour assurer qu'ils restent pertinents et appropriés pour les fournisseurs de services ? [4.4.14 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question à répondre	Réponse	État de mise en œuvre
Composant 3 — ASSURANCE DE LA SÉCURITÉ PAR L'ÉTAT			
Élément 3.1 — Supervision de la sécurité			
3.1-1	[État] a-t-il établi un programme officiel de surveillance pour assurer que les fournisseurs de services se conforment de façon satisfaisante aux règlements et aux exigences de sécurité de l'État ? [4.2.1, Élément 3.1]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-2	[État] a-t-il] établi un processus pour l'examen initial et l'acceptation du SGS d'un fournisseur de services ? [4.2.1, Élément 2.2 ; 4.4.11 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-3	[État] a-t-il établi des procédures pour l'examen des performances des indicateurs de sécurité des différents fournisseurs de services et de leurs niveaux d'alerte/cibles pertinents ? [4.2.1, Élément 2.2 ; 4.4.13]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-4	Le programme de supervision de la sécurité de l'[État] prévoit-il des évaluations périodiques du SGS des différents fournisseurs de services ? [4.2.1, Élément 3.1 ; 4.4.14]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-5	Le programme de surveillance périodique des SGS de l'[État] comprend-il une évaluation des procédures de détection des dangers et de gestion des risques de sécurité des fournisseurs de services ? [4.4.14 c)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-6	Le programme de surveillance périodique des SGS de l'[État] comprend-il une évaluation des performances des indicateurs de sécurité des fournisseurs de services et de leurs niveaux d'alerte/cible pertinents ? [4.4.14 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-7	[État] dispose-t-il d'un mécanisme d'examen périodique interne pour assurer la conformité effective au PNS et ses fonctions connexes de supervision de la sécurité ? [4.4.15]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 3.2 — Collecte, analyse et échange des données de sécurité			
3.2-1	[État] a-t-il établi des mécanismes pour assurer la soumission obligatoire de rapports, l'évaluation et le traitement des données d'accidents et d'incidents graves au niveau global de l'État ? [4.2.1, Élément 3.2 ; 4.4.12]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question à répondre	Réponse	État de mise en œuvre
3.2-2	[État] a-t-il établi un système de compte rendu volontaire pour faciliter la collecte de données sur les dangers et les risques associés de sécurité qui pourraient avoir échappé à un système de compte rendu obligatoire ? [4.4.16 a)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.2-3	[État] a-t-il établi des mécanismes pour établir des informations à partir des données entreposées et pour promouvoir l'échange d'informations de sécurité avec les fournisseurs de services et/ou d'autres États, selon le cas ? [4.2.1, Élément 3.2 ; 4.4.16]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.2-4	[État] a-t-il établi un niveau acceptable de performances de sécurité (ALoSP) défini par des indicateurs de sécurité sélectionnés avec des niveaux d'alerte et de cible appropriés ? [4.4.12 b) ; 4.4.16 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.2-5	Les ALoSP des indicateurs de sécurité sont-ils appropriés et pertinents à l'ampleur et la complexité des activités aéronautiques ? [4.4.12 b) ; 4.4.16 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.2-6	[État] dispose-t-il d'un mécanisme pour la surveillance périodique des indicateurs de sécurité du PNS afin d'assurer l'application de mesures correctives ou de suivi en cas de tendances non souhaitables, de dépassement des niveaux d'alerte ou de non réalisation des cibles d'amélioration ? [4.4.12 b) ; 4.4.16 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 3.3 — Ciblage fondé sur les données de sécurité pour la supervision des domaines présentant de plus grands problèmes ou besoins			
3.3-1	[État] a-t-il établi des procédures pour prioriser les inspections, les audits et les enquêtes visant les domaines présentant de plus grands problèmes ou besoins ? [4.2.1, Élément 3.3 ; 4.4.17]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.3-2	La priorisation des inspections et des audits est-elle liée à l'analyse des données internes/externes de sécurité ou de qualité ? [4.2.1, Élément 3.3 ; 4.4.17]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Composant 4 — PROMOTION DE LA SÉCURITÉ PAR L'ÉTAT			
Élément 4.1 — Formation, communication et diffusion à l'interne d'informations de sécurité			
4.1-1	Y a-t-il un processus pour identifier les besoins de formation liés à la gestion de la sécurité, notamment dans le cadre du PNS et des SGS, à l'intention du personnel compétent des organisations de réglementation/administration ? [4.4.18]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question à répondre	Réponse	État de mise en œuvre
4.1-2	Y a-t-il des registres indiquant que le personnel participant à la mise en œuvre du PNS et à son fonctionnement a reçu une formation ou une familiarisation appropriée au PNS/SGS ? [4.2.1, Élément 4.1 ; 4.4.18]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.1-3	[État] maintient-il un mécanisme pour le regroupement, la communication et le partage des informations de sécurité parmi ses organisations de réglementation et d'administration du PNS ? [4.4.18 d)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.1-4	Le partage à l'interne des informations/données de sécurité comprend-il des rapports sur les événements, les enquêtes et les dangers provenant de tous les secteurs aéronautiques de l'État ? [4.4.16 c)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 4.2 — Formation, communication et diffusion à l'externe d'informations de sécurité			
4.2-1	[État] facilite-t-il la formation continue, la communication et le partage des informations de sécurité avec et entre les fournisseurs de services ? [4.2.1, Élément 4.2 ; 4.4.19]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.2-2	Les organisations de réglementation de l'[État] participent-elles au partage et à l'échange d'informations de sécurité régionales et mondiales et facilitent-elles la participation de leurs fournisseurs de services à ces activités ? [4.4.19 d)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.2-3	Y a-t-il un processus formel pour la diffusion à l'externe de documents et de renseignements de réglementation aux fournisseurs de services et un moyen d'en assurer l'efficacité ? [4.4.19 a)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.2-4	Le document du PNS de l'[État] et ses politiques de sécurité connexes, d'application de la loi et les indicateurs globaux de sécurité sont-ils inclus dans les processus de communication et de partage d'informations de sécurité ? [4.4.19 a)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

2. ANALYSE DÉTAILLÉE DE L'ÉCART ET TÂCHES DE MISE EN ŒUVRE (TABLEAU 4-A7-2)

La liste de vérification de l'analyse initiale de l'écart présentée au Tableau 4-A7-1 devrait alors être suivie de l'utilisation de l'analyse détaillée de l'écart et du plan d'identification des tâches de mise en œuvre figurant dans le Tableau 4-A7-2. Une fois terminé, ce tableau permettra l'analyse de suivi des détails sur les écarts et leur transformation en tâches et sous-tâches effectives requises dans le contexte particulier de l'environnement, des procédures et de la terminologie de l'État. En conséquence, chaque tâche sera attribuée à des personnes ou des groupes appropriés aux fins d'exécution. Il importe que la corrélation de l'établissement des différents éléments/tâches avec leurs signets descriptifs dans le document du PNS soit prise en compte dans le Tableau 4-A7-2, afin de déclencher une mise à jour progressive du projet de document du PNS, à mesure de l'exécution ou du renforcement de chaque élément. (La description initiale des éléments dans les documents de PNS relève plus souvent de l'anticipation que de la constatation.)

3. CALENDRIER DE MISE EN ŒUVRE DES MESURES/TÂCHES (TABLEAU 4-A7-3)

Le Tableau 4-A7-3 montre les étapes principales (dates de commencement/fin) prévues pour chaque mesure/tâche. Dans le cas d'une mise en œuvre par étape, ces mesures/tâches doivent être réparties selon la phase d'allocation des éléments connexes. Voir au besoin la Section 4.4 du présent chapitre. Le Tableau 4-A7-3 peut présenter séparément un regroupement de toutes les mesures/tâches restantes ou, si l'on préfère, une continuation du Tableau 4-A7-2 sous forme de chiffré.

Tableau 4-A7-2. Exemple d'analyse de l'écart et de plan d'identification des tâches de mise en œuvre

<i>Référence GAQ</i>	<i>Question de l'analyse de l'écart</i>	<i>Réponse (Oui/Non/ En partie)</i>	<i>Description de l'écart</i>	<i>Mesure/tâche requise pour combler l'écart</i>	<i>Groupe/personne chargé de la tâche</i>	<i>Référence document PNS</i>	<i>Situation de la mesure/tâche (ouverte/WIP/close)</i>
1.1-1	[État] a-t-il promulgué un cadre législatif national de la sécurité et des règlements particuliers définissant la gestion de la sécurité dans l'État ?	En partie	Aucune définition claire ou attribution des rôles de gestion de la sécurité dans les organisations de réglementation existantes.	Tâche #1 — les services juridiques examineront le cadre législatif	Groupe A	Chapitre 2, Section 1	WIP
1.1-2	Le cadre législatif et les règlements particuliers sont-ils revus périodiquement pour en assurer la pertinence pour l'État ?	En partie	Examen ad hoc ou irrégulière seulement. Aucune SOP pour le processus d'examen périodique.	Tâche #3 — Établir une SOP pour l'examen périodique de tous les règlements d'exploitation	Groupe B	Chapitre 2, Section 3	Ouverte
etc.							

Note.— Le tableau peut contenir toutes les questions de l'analyse de l'écart ou seulement celles qui appellent des réponses « non/en partie », selon les circonstances.

Tableau 4-A7-3. Exemple de calendrier de mise en œuvre des mesures/tâches

Mesure/tâche requis pour combler l'écart	Référence GAQ	Groupe/personne chargé de la tâche	Situation de la mesure/tâche	Calendrier/schéma chronologique (début-fin)												
				1T10	2T10	3T10	4T10	1T11	2T11	3T11	4T11	1T12	2T12	3T12	4T12	etc.
Tâche #1 — les services juridiques examineront le cadre législatif	1.1-1	Groupe A	WIP													
Tâche #2 — Définir la portée du SGS		Groupe 3														
etc.																

Note.— Le Tableau 4-A7-3 peut présenter un regroupement distinct ou, si l'on préfère, une continuation du Tableau 4-A7-2 (chiffrier). S'il est nécessaire de prioriser l'exécution des tâches, voir la Section 4.4 du présent chapitre.

Appendice 8 au Chapitre 4

EXEMPLE DE CONTENU D'UN DOCUMENT DE PNS

TABLE DES MATIÈRES

Page

Liste des amendements	
Avant-propos (par le DGCA/Ministre)	
Tour d'horizon (du document PNS)	
Abréviations/définitions.....	
Chapitre 1. Système national de réglementation de l'aviation	
Chapitre 2. Politiques et objectifs de sécurité de l'État	
2.1 Cadre législatif national de la sécurité	
2.1.1 Législation principale	
2.1.2 Législation auxiliaire	
2.1.3 Règlements/exigences de fonctionnement.....	
2.1.4 Éléments d'orientation de l'industrie	
2.1.5 Cadre et responsabilités de l'Autorité de l'aviation civile	
2.1.6 Examen du cadre/des règlements	
2.1.7 Documents et registres du PNS	
2.2 Responsabilité et imputabilités de l'État en matière de sécurité.....	
2.2.1 Établissement du PNS.....	
2.2.2 Responsabilités et ressources.....	
2.2.3 Comité national de coordination du PNS	
2.2.4 Politique nationale de sécurité.....	
2.2.5 Niveau acceptable de la sécurité	
2.2.6 Amélioration/révision du PNS	
2.3 Enquête sur les accidents et incidents à l'échelle nationale	
2.4 Politique nationale d'application	
Chapitre 3. Gestion des risques de sécurité à l'échelle nationale.....	
3.1 Exigences de sécurité pour les SGS des fournisseurs de services	

3.1.1	Exigences du SGS pour les exploitants aériens et l'organisation approuvée de la maintenance
3.1.2	Exigences POA/DOA du SGS
3.1.3	Exigences du SGS pour les exploitants d'aérodrome.....
3.1.4	Exigences du SGS pour les exploitants ANS
3.1.5	Exigences du SGS pour les ATO
3.2	Approbation des produits ou des performances de sécurité des fournisseurs de services
3.3	Évaluation périodique des produits ou des SGS des fournisseurs de services
Chapitre 4.	Assurance de la sécurité par l'État.....
4.1	Supervision de la sécurité
4.1.1	Systèmes de certification, d'approbation et d'octroi de licences.....
4.1.2	Supervision de la sécurité des produits et des fournisseurs de services.....
4.1.3	Examen à l'interne/assurance de la qualité du PNS.....
4.1.4	Examen à l'externe/audit du PNS.....
4.2	Collecte, analyse et échange des données de sécurité.....
4.2.1	Système de comptes rendus d'événements.....
4.2.2	Système de comptes rendus volontaires/confidentiels
4.3	Ciblage fondé sur les données de sécurité pour la supervision des domaines présentant des problèmes ou besoins plus importants.....
Chapitre 5.	Promotion de la sécurité par l'État
5.1	Formation, communication et diffusion à l'interne d'informations de sécurité.....
5.1.1	Formation à l'interne au PNS, au SGS et à la sécurité.....
5.1.2	Communication et diffusion à l'interne d'informations de sécurité
5.2	Formation, communication et diffusion à l'externe d'informations de sécurité.....
5.2.1	Facilitation de la formation/éducation à l'externe sur les PNS et SGS
5.2.2	Communication et diffusion à l'externe d'informations de sécurité
Appendice 1	— Énoncé de la politique nationale sur la sécurité
Appendice 2	— Énoncé de la politique nationale d'application
Appendice 3	— Plan de mise en œuvre du PNS.....
Appendice 4	— Indicateurs de sécurité et ALOSP nationaux.....

Appendice 9 au Chapitre 4

EXEMPLE DE RÈGLEMENT NATIONAL SUR LES SGS

1. BASE LÉGISLATIVE

Le règlement sur les SGS devrait être promulgué en vertu de l'autorité législative de l'autorité compétente de l'aviation civile de l'État.

2. PORTÉE DU RÈGLEMENT SUR LES SGS

2.1 Le règlement stipule l'obligation pour les fournisseurs de services de mettre en œuvre un système de gestion de la sécurité (SGS) fonctionnant conformément aux dispositions de l'Annexe 1 — *Licences du personnel* ; de l'Annexe 6 — *Exploitation technique des aéronefs* ; de l'Annexe 8 — *Navigabilité des aéronefs* ; de l'Annexe 11 — *Services de la circulation aérienne* ; et de l'Annexe 14 — *Aérodromes, Volume I — Conception et exploitation technique des aérodromes*.

2.2 Dans le contexte de ce règlement, le terme « fournisseur de services » désigne normalement des organisations approuvées/certifiées assurant des services d'aviation. Le terme couvre les institutions de formation approuvées qui sont exposées aux risques opérationnels de sécurité durant la prestation de leurs services, les exploitants d'aéronefs, les organismes de maintenance approuvés, les organisations responsables de la définition de types et/ou de la construction d'aéronefs, les fournisseurs de services de la circulation aérienne et les aérodromes certifiés, selon le cas.

2.3 Le règlement vise les processus, les procédures et les activités aéronautiques liées à la sécurité aérienne des fournisseurs de services, plutôt que la sécurité au travail, la protection de l'environnement ou autres activités non liées à l'aviation.

2.4 Le règlement établit les exigences minimales du cadre SGS. Le fournisseur de services est libre d'imposer des exigences internes plus strictes.

3. EXEMPLE D'UNE CLAUSE DE RÈGLEMENT/EXIGENCE D'UN SGS

3.1 Avec effet au [Date(s)], le [Type de fournisseur de services] devra avoir mis en place un système de gestion de la sécurité (SGS) acceptable à [Nom de l'AAC] et visant les quatre objectifs de sécurité de haut niveau suivants :

- a) identifier les risques de sécurité ;
- b) assurer la mise en œuvre des mesures correctrices requises pour maintenir les performances de sécurité convenues ;
- c) assurer la surveillance continue et l'évaluation régulière des performances de sécurité ;

d) viser à améliorer continuellement les performances générales du système de gestion de la sécurité.

3.2 Le cadre de ce SGS inclura au minimum les composants et éléments ci-après :

1. Politique et objectifs de sécurité
 - 1.1 Engagement et responsabilité de la gestion
 - 1.2 Imputabilités de la sécurité
 - 1.3 Nomination de personnel de sécurité clé
 - 1.4 Coordination de la planification des réponses d'urgence
 - 1.5 Documentation du SGS
2. Gestion des risques de sécurité
 - 2.1 Identification des dangers
 - 2.2 Évaluation et atténuation des risques de sécurité
3. Assurance de la sécurité
 - 3.1 Supervision et mesure des performances de sécurité
 - 3.2 Gestion du changement
 - 3.3 Amélioration continue du SGS
4. Promotion de la sécurité
 - 4.1 Formation et éducation
 - 4.2 Communication sur la sécurité.

Note.— Un règlement sur les SGS devrait être accompagné également de la publication par l'État d'éléments d'orientation ou de textes consultatifs sur les SGS. Ces éléments d'orientation devraient aussi inclure toute disposition sur une méthode de mise en œuvre de SGS par étape. La procédure d'acceptation du SGS d'un fournisseur de services par l'AAC et d'approbation de ses performances de sécurité proposées devrait aussi figurer dans les éléments d'orientation appropriés.

Appendice 10 au Chapitre 4

EXEMPLE DE POLITIQUE NATIONALE D'APPLICATION

Cette politique d'application est promulguée au titre de l'autorité législative indiquée dans les [règlements d'aviation civile, les ordonnances sur la navigation aérienne ou les normes réglementaires applicables de l'État].

1. OBJET

1.1 La politique d'application de l'[AAC de l'État] vise à promouvoir la conformité aux règlements et exigences de sécurité aérienne par des fonctions d'exécution appliquées de façon équitable.

1.2 La mise en œuvre des systèmes de gestion de la sécurité (SGS) exige que l'[AAC de l'État] suive une approche d'application équitable et discrétionnaire afin d'appuyer le cadre PNS-SGS.

1.3 Les politiques et procédures d'application de l'[AAC de l'État] permettront aux fournisseurs de services de considérer et de résoudre à l'interne certains événements incluant des écarts de sécurité, dans le contexte de leurs SGS et à la satisfaction des autorités. Les infractions intentionnelles à la [Loi sur l'aviation civile de l'État] et aux [règlements sur l'aviation civile de l'État] feront l'objet d'enquêtes et, peut-être, de mesures conventionnelles d'application, s'il y a lieu. Il devrait y avoir des dispositions claires dans le cadre de l'application des lois destinées à un examen approprié afin de distinguer entre les infractions préméditées et les erreurs ou les écarts non intentionnels.

1.4 L'énoncé de la politique d'application et les procédures d'exécution connexes s'appliquent aux fournisseurs de services travaillant en conformité à l'Annexe 1 — *Licences du personnel* ; l'Annexe 6 — *Exploitation technique des aéronefs*, Partie I — *Aviation de transport commercial international — Avions*, et Partie III — *Vols internationaux d'hélicoptères* ; l'Annexe 8 — *Navigabilité des aéronefs* ; l'Annexe 11 — *Services de la circulation aérienne* ; et l'Annexe 14 — *Aérodromes*, Volume I — *Conception et exploitation technique des aérodromes*.

2. POLITIQUE

2.1 [Tous les fournisseurs de services admissibles] établiront, maintiendront et appliqueront un SGS qui est proportionnel à l'ampleur, à la nature et à la complexité des exploitations autorisées en vertu de son approbation/certificat.

2.2 Afin de maintenir cette politique d'application à l'appui de la mise en œuvre des SGS, les inspecteurs de l'[AAC de l'État] garderont ouverte une voie de communication avec les fournisseurs de services.

2.3 Aucun renseignement provenant des systèmes de collecte et de traitement de données de sécurité (établis dans le cadre d'un SGS) liées à des rapports classés comme confidentiels, volontaires ou de catégorie équivalente, ne sera utilisé comme base de mesure d'application.

2.4 Lorsqu'un fournisseur de services relevant d'un SGS contrevient de façon non intentionnelle à la [Loi sur l'aviation civile ou aux règlements sur l'aviation civile], des procédures d'examen spécifiques seront appliquées. Ces

procédures donneront à l'inspecteur de l'[AAC de l'État] responsable de la supervision du fournisseur de services la possibilité d'engager un dialogue avec l'organisation approuvée du SGS. Ce dialogue a pour objet de convenir de mesures correctrices proposées et d'un plan d'action pour régler efficacement les carences qui ont causé l'infraction et pour donner au fournisseur de services un délai raisonnable pour les mettre en œuvre. Une telle approche vise à encourager et à soutenir un processus efficace de compte rendu où les employés des fournisseurs de services peuvent signaler les carences et les risques de sécurité sans craindre des mesures punitives. Un fournisseur de services peut donc, sans attribuer de blâmes ni craindre des mesures d'application, analyser l'événement et les facteurs organisationnels ou individuels qui auraient pu en être les causes, afin d'incorporer des mesures correctrices susceptibles d'empêcher de nouveaux incidents.

2.5 Par l'intermédiaire de l'inspecteur responsable de la supervision du fournisseur de services, l'[AAC de l'État] évaluera les mesures correctrices proposées par le fournisseur de services et/ou les systèmes en place pour résoudre l'événement à la base de l'infraction. Si les mesures correctrices proposées (incluant toutes mesures disciplinaires internes appropriées) sont jugées satisfaisantes et susceptibles d'empêcher les récidives et d'encourager la conformité future, l'examen de l'infraction devrait donc être clos par le responsable de la réglementation sans autre mesure d'application punitive. Si les mesures correctrices ou les systèmes en place sont jugés non appropriés, l'[AAC de l'État] poursuivra son dialogue avec le fournisseur de services afin d'arriver à une résolution satisfaisante qui évitera des mesures d'application. Par contre, si le fournisseur de services refuse de régler l'événement et d'appliquer des mesures correctrices effectives, l'[AAC de l'État] envisagera de prendre des mesures d'application ou toute autre mesure administrative jugée appropriée.

2.6 Des infractions aux règlements aéronautiques peuvent survenir pour diverses raisons, allant d'une mauvaise interprétation réelle des règlements au mépris de la sécurité aérienne. L'[AAC de l'État] dispose d'un éventail de procédures d'exécution pour s'acquitter effectivement de ses obligations de sécurité en vertu de la [loi applicable de l'État], compte tenu des diverses circonstances. Ces procédures peuvent donner lieu à une gamme diverse de mesures, telles que les suivantes :

- a) counselling ;
- b) formation corrective ; ou
- c) modification, suspension ou annulation des autorisations.

2.7 Les décisions d'application ne doivent pas être influencées par les facteurs suivants :

- a) conflit personnel ;
- b) intérêt personnel ;
- c) considérations telles que le genre, la race, la religion, les points de vue ou l'appartenance politiques ;
ou
- d) le pouvoir personnel, politique ou financier des personnes en cause.

3. PROPORTIONNALITÉ DES RÉACTIONS

Les décisions d'application doivent être proportionnées aux infractions constatées et aux risques de sécurité qu'elles posent, en respectant les trois principes suivants :

- a) l'[AAC de l'État] prendra des mesures contre tous ceux qui s'écartent systématiquement et délibérément des règlements de l'aviation civile ;

- b) l'[AAC de l'État] s'efforcera d'éduquer et de promouvoir la formation ou la supervision de tous ceux qui se montrent résolus à résoudre les carences de sécurité ;
- c) l'[AAC de l'État] fournira les efforts appropriés et équitables pour distinguer entre les infractions préméditées et les erreurs ou les écarts non intentionnels.

4. JUSTICE NATURELLE ET IMPUTABILITÉ

Les décisions d'application doivent :

- a) être justes et suivre le cours normal de la loi ;
- b) être transparentes pour toutes les personnes en cause ;
- c) tenir compte des circonstances de l'affaire et de l'attitude/des actions du fournisseur de services ou des individus pour arriver à une conclusion ;
- d) arriver à des mesures ou des décisions cohérentes dans des circonstances semblables ou similaires ;
- e) être soumises à des examens internes et externes appropriés.

5. EXCEPTIONS

- 5.1 Cette politique n'est pas applicable s'il y a preuve d'une tentative délibérée de cacher la non-conformité.
- 5.2 Cette politique n'est pas applicable si le fournisseur de services n'a pas maintenu un SGS acceptable ou les performances de sécurité convenues.
- 5.3 Cette politique n'est pas applicable si le fournisseur de services est considéré par l'Autorité l'auteur récidiviste d'infractions.
- 5.4 Dans ces circonstances, l'Autorité peut décider de résoudre les cas de non-conformité ou d'infraction en appliquant les procédures d'exécution établies qu'elle jugerait appropriées.

(Signé)

Administrateur responsable du PNS

Appendice 11 au Chapitre 4

LIGNES DIRECTRICES SUR LES PROCÉDURES NATIONALES D'EXÉCUTION DANS UN ENVIRONNEMENT PNS-SGS

1. GÉNÉRALITÉS

Dans le cadre du programme national de sécurité (PNS) de [l'État], l'AAC de [l'État] est responsable de la supervision des détenteurs de certificats fonctionnant dans un environnement SGS. Les procédures d'exécution contiennent des indications pour les entités responsables de la supervision des fournisseurs de services fonctionnant dans un environnement SGS sur la réponse appropriée aux erreurs ou aux infractions. Les procédures d'exécution jouent un rôle de soutien au processus. Toutefois, la décision finale concernant toute question d'exécution du PNS relève de la responsabilité de l'AAC ou de l'administrateur responsable du PNS.

2. APPLICABILITÉ

2.1 Ces procédures s'appliquent aux infractions qui auraient pu être commises par des personnes ou des fournisseurs de services menant des activités dans un environnement PNS-SGS.

2.2 Ces procédures sont en vigueur à compter du [Date].

2.3 Ces procédures seront appliquées par les fournisseurs de services qui ont un SGS accepté par l'AAC ou qui suivent une approche de mise en œuvre par étape du SGS selon un plan de mise en œuvre accepté par l'AAC.

2.4 Si ces fournisseurs de services ou ces personnes n'ont pas démontré qu'ils fonctionnent dans un environnement SGS, des mesures d'exécution peuvent être appliquées sans les avantages des procédures décrits au paragraphe 3.

3. PROCÉDURES

3.1 Afin de déterminer s'il convient de mener une enquête ou une évaluation d'exécution dans un environnement d'exécution, il sera nécessaire pour l'équipe d'enquête ou d'exécution de déterminer l'état de mise en œuvre du SGS du fournisseur de services visé. Cette détermination se fera initialement par des communications entre le groupe d'exécution et l'inspecteur principal responsable de la supervision et de la certification du fournisseur de services en question. Des délibérations pour l'exécution devraient toujours être menées par un groupe d'administrateurs nommés ou désignés, plutôt que par un administrateur unique.

3.2 L'inspecteur principal déterminera si le fournisseur de services est conforme aux critères mentionnés plus haut pour les procédures d'exécution du SGS. Afin de faciliter l'évaluation initiale, l'AAC de [l'État] devrait tenir une liste de l'état de mise en œuvre des SGS des fournisseurs de services. Cette liste, mise à la disposition du personnel d'enquête/d'exécution, aidera les enquêteurs à former leurs décisions concernant l'applicabilité du processus d'évaluation d'enquête/d'exécution.

3.3 Durant la mise en œuvre par étape du SGS des fournisseurs de services, l'AAC de [l'État] peut appliquer les procédures d'exécution du SGS aux fournisseurs de services qui ne disposent pas encore de SGS accepté ou pleinement mis en œuvre, sous réserve de certaines conditions.

3.4 L'AAC de [l'État] exigera au minimum le respect des trois conditions ci-après avant d'appliquer les procédures d'exécution du SGS :

- a) le fournisseur de services dispose d'une procédure interne efficace de signalement des dangers et d'atténuation des risques ;
- b) le fournisseur de services dispose d'une procédure efficace d'enquête et de mesures correctives adaptée à l'ampleur et à la complexité de ses opérations et permettant de déterminer les facteurs de causalité et d'établir des mesures correctives ;
- c) les données de sécurité ou les informations sur l'événement faisant l'objet de l'enquête sont mises à la disposition du groupe d'enquête/d'exécution, qui bénéficie pleinement de la coopération du fournisseur de services ou de la personne intéressée.

Rapport initial d'infraction

3.5 Le personnel d'exécution du secteur de l'aviation devrait mener une analyse préliminaire de tous les cas où une infraction est détectée ou à la réception d'informations sur une infraction éventuelle. Si l'infraction signalée est le résultat ou la recommandation d'un rapport officiel, le groupe d'exécution devra décider si le rapport de l'événement est adéquat pour appuyer des mesures d'exécution.

Évaluation préliminaire

3.6 Sur la base des informations reçues, il convient de se poser les questions suivantes :

- a) Y a-t-il des motifs raisonnables de croire qu'une personne ou une organisation menant des activités dans le cadre d'un SGS ait pu commettre une infraction ?
- b) L'événement est-il de nature telle (p. ex. infraction grossière/répétée) qu'il conviendrait d'envisager des mesures d'exécution ?
- c) Existe-t-il d'autres informations ou preuves, tels que des conditions latentes, des facteurs organisationnels/humains, qu'il convient d'obtenir afin de faciliter le processus décisionnel sur les mesures d'exécution ?

Si ces questions obtiennent des réponses affirmatives, l'inspecteur principal devrait être notifié pour obtenir son accord de procéder à l'évaluation des mesures d'exécution, selon le cas.

Évaluation et recommandation de mesures d'exécution

3.7 Pour établir une mesure administrative (ou autre mesure punitive) appropriée, juste et efficace, le groupe d'exécution devrait se fonder sur un processus objectif qui tienne compte de toutes les conditions sous-jacentes, circonstancielles, environnementales ou latentes connues. Ces éléments devront inclure des facteurs organisationnels, humains ou d'accroissement applicables. Selon le cas, il conviendrait de tenir compte également d'autres facteurs, tels que la question de savoir si la non-conformité est une erreur non voulue ou un acte délibéré.

3.8 Une fois décidée la mesure d'exécution appropriée, le groupe d'exécution devrait formuler la recommandation requise à l'intention de l'administrateur compétent, pour approbation et notification ultérieure des parties prenantes.

Appendice 12 au Chapitre 4

EXEMPLE DE LISTE DE VÉRIFICATION D'UNE ACCEPTATION/ ÉVALUATION RÉGLEMENTAIRE DE SGS

1. Le Tableau 4-A12-1 est un exemple de liste de vérification d'une évaluation réglementaire de SGS (85 questions) qui peut être utilisé pour l'évaluation et l'acceptation initiales du SGS d'un fournisseur de services. Dans le cas d'une acceptation initiale, les questions d'évaluation doivent être détaillées pour couvrir adéquatement tous les éléments SGS de l'organisation. Ceci permettra de vérifier que tous les éléments et leurs procédures correspondantes sont en place au sein de l'organisation. Il serait plus approprié d'aborder les aspects opérationnels du SGS durant l'évaluation régulière/annuelle ultérieure du SGS.
2. La procédure de performance minimale acceptable prévoit des critères de pointage minimaux acceptables en trois étapes. Pour l'organe de réglementation, une telle procédure facilite l'évaluation progressive du processus de mise en œuvre du SGS du fournisseur de services, au lieu d'attendre la mise en œuvre totale du SGS du fournisseur de services ou sa maturité pour procéder à son audit. Ce protocole d'évaluation progressive permet en outre d'assurer que l'organe de réglementation participe activement à la surveillance de la mise en œuvre des SGS de l'industrie dès les premières phases.
3. Dans le cas d'une mise en œuvre par étape des éléments du SGS, décrite dans le Chapitre 5 du présent document, les questions de la liste de vérification pourraient nécessiter une nouvelle configuration et une adaptation pour les aligner sur l'aménagement particulier des éléments dans les diverses phases pertinentes, selon la détermination de l'État.
4. On trouvera à la fin de la liste de vérification une procédure illustrative d'avis d'action corrective (CAN).
5. Le Tableau 4-A12-2 est un exemple de liste de vérification d'une évaluation réglementaire de SGS (39 questions) pouvant être utilisé pour une évaluation ultérieure de routine de SGS. Une fois que le SGS d'une organisation a répondu au processus d'évaluation et d'acceptation initiales, il restera de nombreuses questions d'évaluation de la liste de vérification initiale qu'il ne serait plus pratique ni utile d'appliquer pour l'évaluation de routine. Pour une telle évaluation, la liste de vérification doit simplement se concentrer sur les aspects opérationnels d'un SGS et déterminer la mise en œuvre satisfaisante de ses procédures de soutien.
6. Une évaluation de routine du SGS peut être menée de façon autonome ou être incorporée à l'audit de routine de l'organisation ou du système. Dans ce dernier cas, les questions de l'évaluation de routine peuvent être incorporées comme une section de la liste de vérification de l'audit normal de l'organisation. Le vérificateur exécutant un audit intégré QMS-SGS devra être formé comme il faut à l'audit des SGS. Le protocole normal d'avis d'action corrective (CAN) de l'organe de réglementation peut également s'appliquer à l'évaluation de routine du SGS.

Tableau 4-A12-1. Liste de vérification de l'évaluation du SGS — Acceptation initiale du SGS

Liste de vérification de l'évaluation du SGS — Acceptation initiale					Liste de vérification d'audit — routine du SGS/18 août 2011				
Colonne « Intransit » : Remplir en inscrivant « Y » pour Oui, « N » pour Non, « N/A » pour Sans objet									
Nom de l'organisation :			Date de l'évaluation :			Évalué par POI/PMI :			Réf. :
Élément	Niveau 1	Intransit	Réf. Doc/ remarques	Niveau 2	Intransit	Réf. Doc/ remarques	Niveau 3	Intransit	Réf. Doc/ remarques
Engagement et responsabilités de gestion [1.1]	Composant 1. Politique et objectifs de sécurité								
	1.1/L1/1		Y	1.1/L2/1		N	1.1/L3/1		N
	Il y a un énoncé de politique documenté sur la sécurité.			Il y a preuve que la politique de sécurité est communiquée à tous les employés, dans le but de leur faire prendre conscience de leurs obligations individuelles en matière de sécurité.			Il y a un examen périodique de la politique de sécurité par la haute direction ou le comité de la sécurité.		
	1.1/L1/2		Y	1.1/L2/2		Y	1.1/L3/2		N
	La politique de sécurité est pertinente à la sécurité de l'aviation.			La politique de sécurité est approuvée par le gestionnaire responsable.			Le mandat du gestionnaire responsable indique sa responsabilité générale pour toutes les questions de sécurité.		
	1.1/L1/3		N	1.1/L2/3		N			
La politique de sécurité est pertinente à l'ampleur et à la complexité des opérations de l'organisation.		La politique de sécurité comprend la fourniture des ressources humaines et financières nécessaires à sa mise en œuvre.		—					
Imputabilités de sécurité [1.2]	1.2/L1/1		Y	1.2/L2/1		N			
	Il y a au sein de l'organisation une imputabilité de sécurité documentée (SGS), qui commence avec le gestionnaire responsable.			Le mandat du gestionnaire responsable indique sa responsabilité ultime de la gestion de la sécurité de son organisation.			—		
	1.2/L1/2		N	1.2/L2/2		N			
L'administrateur responsable a l'autorité finale sur toutes les activités aéronautiques de son organisation.		Le mandat du gestionnaire responsable indique son autorité finale sur toutes les opérations menées au titre du(des) certificat(s) de son organisation.		—					

Élément	Niveau 1	Intrant	Réf. Doc/ remar- ques	Niveau 2	Intrant	Réf. Doc/ remar- ques	Niveau 3	Intrant	Réf. Doc/ remarques
Imputabilités de sécurité [1.2]	1.2/L1/3			1.2/L2/3			1.2/L3/1		
	Il y a un comité de la sécurité (ou un mécanisme équivalent) qui examine le SGS et ses performances de sécurité.	Y		Dans le cas d'une grande organisation, il existe, au niveau des départements ou des sections, des groupes d'action pour la sécurité qui travaillent en conjonction avec le comité de la sécurité.	N/A		Le comité de la sécurité est présidé par le gestionnaire responsable ou (pour les très grandes organisations) par un suppléant dûment attiré et documenté dans le manuel du SGS.	Y	
	1.2/L1/4			1.2/L2/4			1.2/L3/2		
	Le comité de la sécurité comprend des chefs opérationnels ou des chefs de service, selon qu'il convient.	N		Le groupe d'action pour la sécurité comprend un coordonnateur de sécurité dûment désigné (SGS).	N/A		Les groupes d'action pour la sécurité sont présidés par le chef de département ou de section, selon le cas.	N/A	
Nominations de personnel de sécurité clé [1.3]	1.3/L1/1			1.3/L2/1			1.3/L3/1		
	Il y a un gestionnaire qui assure le rôle d'administration du SGS.	Y		Le gestionnaire responsable de l'administration du SGS n'a pas d'autre responsabilité qui risque de compromettre ou d'entrer en conflit avec son rôle de gestionnaire du SGS.	N		Le gestionnaire du SGS a un accès direct ou rend compte directement au gestionnaire responsable pour la mise en œuvre et le fonctionnement du SGS.	N	
	1.3/L1/2			—			1.3/L3/2		
	Le mandat du gestionnaire assurant le rôle d'administration du SGS indique ses fonctions pertinentes concernant le SGS.	N					Le gestionnaire du SGS occupe un poste de la haute direction, qui n'est ni inférieur ni subordonné à d'autres postes d'exploitation ou de production.	N	
Planification de la riposte d'urgence [1.4]	1.4/L1/1			1.4/L2/1			1.4/L3/1		
	Il y a un ERP documenté ou une procédure opérationnelle de contingence équivalente.	Y		L'ERP comprend des procédures pour la sécurité continue de la production, de la livraison ou du soutien des produits ou services aéronautiques durant les situations d'urgence ou de contingence.	N		L'ERP prévoit une intégration pertinente avec des organisations externes de clients ou de sous-traitants, selon le cas.	N	
	1.4/L1/2			1.4/L2/2			1.4/L3/2		
	L'ERP est approprié pour la taille, la nature et la complexité de l'organisation.	Y		Des exercices d'entraînement sont prévus pour l'ERP.	Y		Il y a une procédure pour l'examen périodique de l'ERP, afin d'en assurer la pertinence et l'efficacité continues.	N	
	1.4/L1/3			1.4/L2/3					
	Le plan d'urgence prévoit des scénarios d'urgence ou de crise possible ou probable liés à la livraison de produits ou de services aéronautiques de l'organisation.	N		Des exercices d'entraînement pour l'ERP sont exécutés conformément au plan et les résultats de ces exercices sont documentés.	N		—		

Élément	Niveau 1	Intrant	Réf. Doc/ remar- ques	Niveau 2	Intrant	Réf. Doc/ remar- ques	Niveau 3	Intrant	Réf. Doc/ remarques
Documentation SGS [1.5]	1.5/L1/1			1.5/L2/1			1.5/L3/1		
	Il y a un document ou une présentation du SGS qui est approuvé par le gestionnaire responsable et accepté par l'AAC.	Y		Le document du SGS est accepté ou entériné par l'autorité de l'aviation nationale de l'organisation.	Y		Les procédures du SGS tiennent compte de l'intégration appropriée avec d'autres systèmes de gestion pertinents au sein de l'organisation, tels que QMS, OSHE, sûreté, selon le cas.	N	
	1.5/L1/2			1.5/L2/2			1.5/L3/2		
	Le document du SGS donne un tableau général ou une présentation du cadre et des éléments du SGS de l'organisation.	Y		La présentation de chaque élément dans le document du SGS comprend des renvois à des procédures, des manuels ou des systèmes connexes ou de soutien, selon le cas.	Y		Les procédures du SGS tiennent compte de la coordination ou de l'intégration pertinente avec des organisations de clients ou de sous-traitants externes, selon le cas.	N	
	1.5/L1/3			1.5/L2/3			1.5/L3/3		
	Le document du SGS est un document autonome contrôlé ou une partie/section distincte d'un document accepté/entériné par l'AAC.	Y		Des registres sont maintenus concernant les procès-verbaux des réunions du Comité de la sécurité/SAG (ou l'équivalent).	Y		Il existe une procédure d'examen périodique de la présentation du SGS et des documents de soutien, afin d'en assurer la pertinence continue.	N	
	1.5/L1/4			1.5/L2/4					
	Tous les composants et éléments des dispositions réglementaires du SGS sont abordés dans le document du SGS.	Y		Les registres concernant l'examen périodique des évaluations existantes de sécurité ou de risques ou des examens spéciaux liés aux changements pertinents sont disponibles.	N		—		
	1.5/L1/5								
	Des registres sont maintenus sur les évaluations des risques effectuées.	Y		—			—		
1.5/L1/6									
Des registres sont maintenus sur les risques/menaces détectés ou signalés.	Y		—			—			

Élément	Niveau 1	Intrant	Réf. Doc/ remar- ques	Niveau 2	Intrant	Réf. Doc/ remar- ques	Niveau 3	Intrant	Réf. Doc/ remarques
Détection des risques [2.1]	Composant 2. Gestion des risques de sécurité								
	2.1/L1/1		Y	2.1/L2/1		N	2.1/L3/1		N
	Il y a une procédure pour la soumission volontaire de comptes rendus des risques/menaces par tous les employés.			Le système de détection des risques définit et distingue clairement les risques et leurs conséquences.			Il y a une procédure pour identifier les risques/menaces dans les rapports internes d'accident/incident, aux fins d'atténuation durant le suivi, selon le cas.		
	2.1/L1/2		Y	2.1/L2/2		N	2.1/L3/2		N
	Il y a une procédure de compte rendu des incidents/accidents par le personnel d'exploitation ou de production.			Le système de compte rendu des risques est confidentiel et comprend des dispositions pour protéger l'identité des auteurs de comptes rendus.			Il y a une procédure pour examiner les risques/menaces indiqués dans les rapports de service ou d'incident/accident pertinents de l'industrie, aux fins d'atténuation de ces risques, le cas échéant.		
2.1/L1/3		Y	2.1/L2/3		N	2.1/L3/3		N	
Il y a une procédure d'enquête sur les incidents/accidents liée à la qualité ou à la sécurité.			Les procédures d'enquête et de discipline internes de l'organisation font la distinction entre les infractions préméditées et délibérées et les erreurs/fautes non intentionnelles.			Il y a une procédure pour l'examen périodique des registres existants des analyses de risques.			
Évaluation et atténuation des risques de sécurité [2.2]	2.2/L1/1		Y	2.2/L2/1		N	—		
	Il y a une procédure HIRM documentée couvrant le recours aux outils d'analyse objective des risques.			Les rapports d'évaluation des risques sont approuvés par les directeurs des départements ou à un niveau plus élevé, selon le cas.					
	2.2/L1/2		N	2.2/L2/2		N	—		
	Il y a une procédure pour l'identification des opérations, des processus, des services et installations et des équipements qui sont considérés (par l'organisation) comme pertinents pour la HIRM.			Les mesures d'atténuation recommandées qui doivent être décidées ou approuvées par la haute direction font l'objet de rapport et sont documentées.					
2.2/L1/3		N	2.2/L2/3		N	2.2/L3/1		N	
Il y a un programme pour la performance progressive HIRA de tous les opérations, processus, services et installations et équipements identifiés par l'organisation comme étant liés à la sécurité aérienne.			Il y a une procédure pour la priorisation des applications de l'HIRA pour les opérations, les processus, les services et installations et les équipements présentant des dangers/risques de sécurité critiques identifiés ou connus.			Il y a preuve de la conformité progressive et du maintien du programme d'application HIRA de l'organisation.			

Élément	Niveau 1	Intrant	Réf. Doc/ remar- ques	Niveau 2	Intrant	Réf. Doc/ remar- ques	Niveau 3	Intrant	Réf. Doc/ remarques
Surveillance et mesure des performances de sécurité [3.1]	Composant 3. Assurance de la sécurité								
	3.1/L1/1			3.1/L2/1			3.1/L3/1		
	Il y a des indicateurs de performance de sécurité identifiés pour la mesure et la surveillance des performances de sécurité de l'organisation.	Y		Il y a des indicateurs de performance de sécurité à faibles conséquences (p. ex. non-conformité, écarts).	N		Il y a une procédure pour l'application de mesures correctrices ou de suivi lorsque les cibles ne sont pas atteintes et/ou lorsque le niveau d'alerte est dépassé.	N	
	3.1/L1/2			3.1/L2/2			3.1/L3/2		
Il y a des indicateurs de performance de sécurité fondés sur des données à conséquences élevées (p. ex. taux d'accident et d'incident grave).	Y	Des niveaux d'alerte et/ou de cible sont établis dans les indicateurs de performance de sécurité, selon le cas.		N	Les performances des indicateurs de sécurité sont examinées par le Comité de la sécurité pour détecter les tendances, les dépassements des niveaux d'alerte, la réalisation des cibles, le cas échéant.		Y		
La gestion des changements [3.2]	3.2/L1/1			3.2/L2/1			3.2/L3/1		
	Il y a une procédure pour l'examen des services, installations et équipements existants liés à la sécurité aérienne (incluant des registres HIRA) chaque fois que des changements pertinents sont apportés à ces services, installations ou équipements	N		Il y a une procédure pour l'examen des nouveaux services/installations et équipements liés à la sécurité de l'aviation afin d'en détecter les dangers/risques avant leur mise en service.	N		Il y a une procédure pour l'examen des services et installations, des équipements, des opérations ou des processus pertinents existants (incluant des registres HIRM), chaque fois qu'il y a des changements pertinents extérieurs à l'organisation, tels que des normes réglementaires/de l'industrie, des meilleures pratiques ou des technologies.	N	
	3.2/L1/2			3.2/L2/2					
	Il y a une procédure pour l'examen des opérations et processus d'aviation existants (incluant des registres HIRA) chaque fois que des changements pertinents sont apportés à ces opérations et processus.	N		Il y a une procédure pour l'examen des nouvelles opérations aéronautiques liées à la sécurité et de nouveaux processus concernant les dangers/risques, préalablement à leur mise en œuvre.	N		—		

Élément	Niveau 1	Intrant	Ref. Doc/ remar- ques	Niveau 2	Intrant	Ref. Doc/ remar- ques	Niveau 3	Intrant	Ref. Doc/ remarques
Amélioration continue du SGS [3.3]	3.3/L1/1			3.3/L2/1			3.3/L3/1		
	Il y a une procédure pour l'audit ou l'évaluation périodique interne du SGS.	Y		Il y a une procédure portant sur les mesures de suivi des audits	Y		L'audit/évaluation du SGS a été mené conformément au plan.	N	
	3.3/L1/2			3.3/L2/2			3.3/L3/2		
	Il y a actuellement un plan pour l'audit/évaluation interne du SGS.	N		-			Il y a un processus pour soumettre au gestionnaire responsable ou pour appeler son attention sur les rapports sur l'audit/évaluation du SGS, lorsque c'est nécessaire.	N	
	3.3/L1/3			3.3/L2/3			3.3/L3/3		
Il y a une procédure documentée pour l'audit/évaluation interne du SGS.	N		Le plan d'audit du SGS prévoit l'échantillonnage d'évaluations de la sécurité réalisées.	N		Le plan d'audit du SGS couvre les rôles/contributions des agents contractuels du SGS, le cas échéant.	N		
Formation et communication [4.1, 4.2]	Composant 4. Promotion de la sécurité								
	4.1/L1/1			4.1/L2/1			4.1/L3/1		
	Il y a une politique documentée de formation/familiarisation du personnel au SGS.	Y		Le personnel participant à l'évaluation des risques a reçu une formation ou une familiarisation appropriée à la gestion des risques.	N		Il y a preuve des efforts d'éducation ou de sensibilisation au SGS à l'échelle de l'organisation.	N	
	4.1/L1/2			4.1/L2/2			4.1/L3/2		
	Le fonctionnaire responsable de l'administration du SGS a suivi un cours approprié de formation au SGS.	Y		Le personnel lié directement au SGS (membres du Comité de la sécurité/SAG) a reçu une formation ou une familiarisation appropriée au SGS.	N		Il y a preuve d'une publication (SGS), d'une circulaire ou d'une voie pour communiquer aux employés sur des questions relatives à la sécurité et au SGS.	N	
4.1/L1/3									
Le gestionnaire responsable a suivi un cours approprié de familiarisation, d'information ou de formation au SGS.	Y		-			-			

TOTAL PARTIEL	CATÉGORIE 1
Y	23
N	11
N/A	0
Nombre de questions remplies	34

CATÉGORIE 2
6
21
2
29

CATÉGORIE 3
2
19
1
22

GRAND TOTAL*	
Y	31
N	51
N/A	3
Nombre de questions remplies	85

RÉSULTAT DE L'ÉVALUATION (% DE OUI) : 38,7 %

PROCÉDURE D'AVIS DE MESURES CORRECTRICES (CAN)

- 1) Performances générales minimales acceptables (mise en œuvre par étape du SGS) :

Première année/étape d'évaluation (p. ex. 2012) — 45 %.

Deuxième année/étape d'évaluation (p. ex. 2013) — 65 %.

Troisième année/étape d'évaluation (p. ex. 2014) et au-delà — 85 %.

Quatre-vingt-dix (90) jours pour appliquer des mesures correctrices afin d'obtenir des performances générales minimales de 45 %.

- 2) Performances de référence (questions du niveau 1) (durant toute année/étape d'évaluation ultérieure à la date d'applicabilité nationale requise du SGS) :

Avis de mesure correctrice (CAN) à émettre pour les réponses négatives à toutes questions du niveau 1 questions (durant toute année/étape d'évaluation).
[Soixante (60) jours pour appliquer des mesures correctrices afin d'obtenir une réponse positive au(x) question(s) pertinente(s)].

Tableau 4-A12-2. Liste de vérification d'évaluation du SGS — Évaluation de routine de SGS

<i>Élément du SGS</i>		<i>Question de l'évaluation</i>
Engagement et responsabilités de gestion [1.1]	1	La politique de sécurité est pertinente à l'ampleur et à la complexité des opérations de l'organisation.
	2	Il y a preuve que la politique de sécurité est communiquée à tous les employés dans le but de leur faire prendre connaissance de leurs obligations individuelles en matière de sécurité.
	3	Il y a un examen périodique de la politique de sécurité par la haute direction ou par le comité de la sécurité.
	4	Le mandat de l'administrateur responsable décrit ses responsabilités générales pour toutes les questions de sécurité.
Imputabilités en matière de sécurité [1.2]	1	Il y a un comité de la sécurité (ou un mécanisme équivalent) qui examine le SGS et ses performances de sécurité.
	2	Le mandat de l'administrateur responsable indique qu'il a l'autorité finale de toutes les opérations menées en vertu des certificats de l'organisation.
Nomination de personnel clé de la sécurité [1.3]	1	Le mandat de l'administrateur assurant le rôle du SGS contient des fonctions SGS pertinentes.
	2	L'administrateur responsable du SGS ne détient aucune autre responsabilité qui pourrait gêner ou entrer en conflit avec son rôle de gestionnaire du SGS.
	3	L'administrateur du SGS a un accès direct ou répond directement du directeur responsable de la mise en œuvre et du fonctionnement du SGS.
	4	L'administrateur du SGS occupe un poste de haute direction qui n'est ni inférieur ni subordonné aux autres postes d'exploitation ou de production.
Planification de la riposte d'urgence (ERP) [1.4]	1	L'ERP couvre les scénarios possibles ou probables d'urgence ou de crise liés à la prestation des services aéronautiques de l'organisation.
	2	L'ERP comprend des procédures pour la sécurité de la poursuite de la production, de la livraison ou du soutien de ses produits ou services durant les situations d'urgence ou imprévues.
	3	Les exercices ou les sessions d'entraînement de l'ERP sont exécutés selon le plan et les résultats des exercices sont documentés.
	4	L'ERP couvre l'intégration d'éléments appropriés avec les organisations de clients ou de sous-traitants externes, si possible.
	5	Il y a preuve d'examen périodique de l'ERP pour en assurer la pertinence et l'efficacité continues.

Élément du SGS		Question de l'évaluation
Documentation du SGS [1.5]	1	Les composants et les éléments du SGS de l'organisation sont pris en compte de façon appropriée dans le document du SGS.
	2	Les composants et éléments documentés du SGS de l'organisation sont conformes aux exigences du SGS de l'autorité de l'aviation.
	3	Il y a preuve de coordination ou d'intégration du SGS pertinent avec les organisations de clients ou de sous-traitants externes, quand c'est possible.
	4	Il y a preuve de procédures d'examen périodique du document de SGS et des documents d'appui pour en assurer la pertinence continue.
	5	Des dossiers concernant l'examen périodique des évaluations existantes de sécurité ou de risques sont disponibles.
Identification des risques [2.1]	1	Le nombre ou le taux des rapports de l'organisation enregistrés ou recueillis sur les risques est proportionnel à l'ampleur et à la complexité des opérations de l'organisation.
	2	Le système de compte rendu des risques est confidentiel et comprend des dispositions destinées à protéger l'identité de l'auteur du compte rendu.
	3	Il y a preuve que les risques/menaces détectés durant l'enquête sur les accidents/incidents sont inscrits dans le système HIRM.
	4	Il y a preuve que les risques inscrits sont examinés systématiquement aux fins d'atténuation si possible.
Évaluation et atténuation des risques de sécurité [2.2]	1	Il y a preuve que les opérations, les procédures, les services et installations et le matériel liés à la sécurité aérienne sont progressivement soumis au processus HIRM de l'organisation.
	2	Les rapports d'évaluation des risques sont approuvés par un niveau approprié de la direction.
	3	Il y a une procédure pour l'examen périodique des dossiers de mesures prises pour l'atténuation des risques.
Surveillance et mesure des performances de sécurité [3.1]	1	Les indicateurs de performance de sécurité du SGS de l'organisation ont été convenus avec l'autorité nationale compétente de l'aviation.
	2	Il y a des indicateurs de performance de sécurité fondés sur des données à conséquences élevées (p. ex. taux d'accident et d'incident grave)
	3	Il y a des indicateurs de performance de sécurité fondés sur des données à faibles conséquences (p. ex. cas de non-conformité, d'écart).
	4	Il y a des niveaux d'alerte et/ou de cible établis dans les indicateurs de performance de sécurité appropriés.
	5	La procédure de gestion des changements de l'organisation comprend l'exigence d'une évaluation des risques à effectuer chaque fois que cela s'applique.

<i>Élément du SGS</i>		<i>Question de l'évaluation</i>
	6	Il y a preuve que des mesures correctrices ou de suivi sont prises lorsque les cibles ne sont pas atteintes ou que des niveaux d'alerte sont dépassés.
La gestion des changements [3.2]	1	Il y a preuve que les processus et opérations pertinents de sécurité aérienne ont été soumis au processus HIRM de l'organisation, le cas échéant.
	2	Les procédures de gestion des changements de l'organisation comprennent l'exigence d'évaluation des risques de sécurité à mener le cas échéant.
Amélioration continue du SGS [3.3]	1	Il y a preuve qu'un audit/une évaluation internes du SGS a été prévu et exécuté.
Formation, éducation et communication [4.1, 4.2]	1	Il y a preuve que tous les employés participant aux opérations du SGS ont reçu une formation ou une familiarisation appropriée sur le SGS.
	2	Le personnel chargé de mener des évaluations des risques a reçu une formation ou une familiarisation appropriée sur la gestion des risques.
	3	Il y a preuve d'une publication (SGS), d'une circulaire ou d'une voie pour communiquer avec les employés sur des questions de sécurité et du SGS.

Chapitre 5

SYSTÈME DE GESTION DE LA SÉCURITÉ (SGS)

5.1 INTRODUCTION

5.1.1 Un SGS est un système conçu pour assurer la sécurité de l'exploitation des aéronefs grâce à une gestion efficace des risques de sécurité. Ce système est conçu pour améliorer constamment la sécurité par l'identification des dangers, la collecte et l'analyse des données et par l'évaluation continue des risques de sécurité. Le SGS vise, de manière proactive, à contenir ou à atténuer les risques avant que ceux-ci n'aboutissent à des accidents et incidents d'aviation. C'est un système qui est adapté aux obligations réglementaires et aux objectifs de sécurité de l'organisation.

5.1.2 L'utilité du SGS est de permettre à un organisme d'aviation d'identifier les dangers et de gérer les risques de sécurité qu'il rencontrera au cours de la fourniture de ses produits et services. Un SGS comprend des éléments clés qui sont essentiels à l'identification des dangers et à la gestion des risques de sécurité en garantissant que :

- a) les renseignements nécessaires sont disponibles ;
- b) les outils appropriés à la tâche sont disponibles pour être utilisés par l'organisation ;
- c) les outils sont appropriés à la tâche à accomplir ;
- d) les outils répondent aux besoins et aux contraintes de l'organisation ;
- e) que les décisions sont prises en tenant pleinement compte du risque de sécurité.

5.2 PORTÉE

Le SGS couvre les activités d'aviation d'un prestataire de services d'aviation qui sont liées à la sécurité de l'exploitation des aéronefs. La portée d'un SGS peut indirectement comprendre d'autres activités de l'organisation qui appuient le développement opérationnel ou le développement de produits, comme les finances, les ressources humaines et les affaires juridiques. Il est donc essentiel de faire participer toutes les parties prenantes internes et externes du système d'aviation qui ont un impact potentiel sur la performance de sécurité de l'organisation. De plus, il convient de tenir compte dès le début de la mise en œuvre d'un SGS et pendant toutes les évaluations internes futures du SGS des concours potentiels dont il peut bénéficier. Les parties prenantes ci-après peuvent apporter leur concours aux prestataires de services selon leur impact potentiel sur la performance de sécurité :

- a) professionnels de l'aviation ;
- b) autorités de réglementation et administratives de l'aviation ;
- c) associations professionnelles de l'industrie ;
- d) associations et fédérations professionnelles ;
- e) organismes internationaux d'aviation ;

- f) sous-contractants ou commettants d'un prestataire de services ;
- g) voyageurs aériens.

5.3 CADRE DU SGS

5.3.1 La présente section présente un cadre pour la mise en œuvre du SGS par les prestataires de services d'aviation pertinents. Il convient de noter que la mise en œuvre du cadre devrait correspondre à la taille de l'organisation et à la complexité des produits ou services fournis.

5.3.2 Le cadre comprend 4 composants et 12 éléments représentant les exigences minimales pour la mise en œuvre du SGS. Les quatre composants d'un SGS sont :

- a) politique et objectifs de sécurité ;
- b) gestion des risques de sécurité ;
- c) assurance de la sécurité ;
- d) promotion de la sécurité.

5.3.3 Ce sont les politiques et objectifs de sécurité qui constituent le cadre de référence pour le SGS. L'objectif du composant gestion des risques de sécurité est d'identifier les dangers, d'évaluer les risques connexes et de développer des atténuations appropriées dans le contexte de la fourniture des produits ou services de l'organisation. L'assurance de sécurité s'obtient dans le cadre de processus permanents qui surveillent le respect des normes internationales et des règlements nationaux. En outre, le processus d'assurance de la sécurité garantit que le SGS fonctionne comme prévu et qu'il est efficace. La promotion de la sécurité offre la sensibilisation et la formation nécessaires.

5.3.4 Le cadre SGS de l'OACI est constitué de 4 composants et 12 éléments, comme suit :

1. Politique et objectifs de sécurité
 - 1.1 Engagement et responsabilité de la direction
 - 1.2 Imputabilités en matière de sécurité
 - 1.3 Nomination du personnel clé de sécurité
 - 1.4 Coordination de la planification des interventions d'urgence
 - 1.5 Documentation relative au SGS
2. Gestion des risques de sécurité
 - 2.1 Identification des dangers
 - 2.2 Évaluation et atténuation des risques de sécurité
3. Assurance de la sécurité
 - 3.1 Surveillance et mesure des performances de sécurité
 - 3.2 La gestion du changement
 - 3.3 Amélioration continue du SGS

4. Promotion de la sécurité

- 4.1 Formation et éducation
- 4.2 La communication relative à la sécurité.

5.3.5 Des détails supplémentaires sur chacun des 4 composants et des 12 éléments sont présentés ci-dessous. Pour chaque composant est fournie une synthèse simple, suivie du texte du cadre du SGS pour chaque élément. Des orientations générales/stratégies de mise en œuvre sont alors présentées pour chaque élément.

Composant 1 du SGS. Politique et objectifs de sécurité

5.3.6 La politique de sécurité énonce les principes, processus et méthodes du SGS de l'organisation pour réaliser les résultats de sécurité souhaités. La politique établit l'engagement de la haute direction d'incorporer et d'améliorer constamment la sécurité dans tous les aspects de ses activités. La haute direction développe des objectifs à réaliser qui sont mesurables et atteignables à l'échelle de l'organisation.

Élément 1.1 du SGS Engagement et responsabilité de la direction

Le prestataire de services définit sa politique de sécurité conformément aux exigences internationales et nationales. La politique de sécurité :

- a) reflétera l'engagement de l'organisation à l'égard de la gestion de la sécurité ;
- b) inclura un énoncé clair au sujet de la fourniture des ressources nécessaires à sa mise en œuvre ;
- c) inclura des procédures de comptes rendus de sécurité ;
- d) indiquera clairement quels types de comportements sont inacceptables dans le cadre des activités d'aviation du prestataire de services et inclura les conditions dans lesquelles une action disciplinaire ne s'appliquerait pas ;
- e) sera signée par le Dirigeant responsable de l'organisation ;
- f) sera communiquée, avec une approbation visible, à travers toute [l'organisation] ;
- g) sera périodiquement réexaminée pour s'assurer qu'elle demeure pertinente et appropriée au prestataire de services.

Orientations générales

5.3.7 Dans toute organisation, la direction a la haute main sur les activités du personnel et l'utilisation des ressources qui sont nécessaires à la fourniture d'un produit ou service. L'exposition de l'organisation à des dangers pour la sécurité est une conséquence de ces activités. La direction atténue les risques de sécurité connexes comme suit :

- a) en établissant les priorités et tâches de l'organisation ;

- b) en prescrivant des procédures sur la façon de réaliser les activités ou processus ;
- c) en recrutant, entraînant et supervisant du personnel ;
- d) en acquérant l'équipement pour appuyer les activités de fourniture de services ;
- e) en utilisant les compétences de son personnel ;
- f) en affectant les ressources nécessaires.

5.3.8 La direction devrait veiller :

- a) à ce que des directives et contrôles en matière de sécurité soient ancrés dans des procédures d'exploitation normalisées (SOP) ;
- b) à ce que les employés respectent les SOP et les directives de sécurité ;
- c) à ce que l'équipement reste en bon état de fonctionnement.

5.3.9 La direction s'acquitte de sa responsabilité principale d'assurer la sécurité et l'efficacité de l'exploitation en veillant au respect des SOP (respect de la réglementation de sécurité) et à la mise en place et à l'exploitation d'un SGS dédié qui établit les contrôles nécessaires des risques de sécurité (performance en matière de sécurité).

Stratégie de mise en œuvre

5.3.10 La haute direction élabore et entérine la politique de sécurité, qui est signée par le Dirigeant responsable (voir Appendice 1 pour une analyse de l'acceptation et de l'utilisation des signatures électroniques dans la politique de sécurité et autres documents connexes du SGS). La Figure 5-1 comprend un exemple d'un énoncé de politique de sécurité.

5.3.11 Une fois que la politique de sécurité a été élaborée, la haute direction devrait :

- a) entériner la politique, de manière visible ;
- b) communiquer la politique à tout le personnel approprié ;
- c) établir pour le SGS et l'organisation des cibles de performance de sécurité ;
- d) établir des objectifs de sécurité qui précisent ce que l'organisation entend réaliser en termes de gestion de la sécurité.

5.3.12 La politique de sécurité doit inclure un engagement :

- a) d'atteindre les plus hautes normes de sécurité ;
- b) de se conformer à toutes les exigences réglementaires applicables ;

ÉNONCÉ DE POLITIQUE DE SÉCURITÉ

La sécurité est une de nos fonctions d'entreprise essentielles. Nous prenons l'engagement d'élaborer, mettre en œuvre, maintenir et améliorer constamment des stratégies et processus devant assurer que toutes nos activités d'aviation auront lieu dans le cadre d'une attribution équilibrée des ressources de l'organisation, visant à réaliser le plus haut niveau de performance de sécurité et à satisfaire aux exigences réglementaires, au cours de la fourniture de nos services.

Tous les échelons de la direction et tous les employés sont responsables de la réalisation de ce haut niveau de performance de sécurité, à commencer par le [directeur général/administrateur gérant/ou titre approprié pour l'organisation].

Nous nous engageons à :

- appuyer la gestion de la sécurité par la fourniture de toutes les ressources appropriées, avec pour résultat une culture organisationnelle qui suscite des pratiques de sécurité, encourage des comptes rendus et une communication de sécurité efficaces, et gère activement la sécurité avec la même attention pour les résultats que celle qui est portée aux résultats des autres systèmes de gestion de l'organisation ;
- veiller à ce que la gestion de la sécurité soit une responsabilité première de tous les cadres et de tous les employés ;
- définir clairement pour tout le personnel, cadres et employés pareillement, ses responsabilités vis-à-vis de la réalisation de la performance de sécurité de l'organisation et de la performance de notre système de gestion de la sécurité ;
- établir et utiliser des processus d'identification des dangers et de gestion des risques, y compris un système de compte rendu de dangers, afin d'éliminer ou d'atténuer les risques de sécurité ou les conséquences de dangers résultant de nos opérations ou activités, afin d'obtenir des améliorations continues de notre performance de sécurité ;
- veiller à ce qu'aucune mesure ne soit prise à l'encontre d'aucun agent qui divulgue une préoccupation de sécurité au travers du système de compte rendu de dangers, à moins que cette divulgation ne révèle, au-delà de tout doute raisonnable, une négligence grossière ou une violation délibérée ou volontaire de règlements ou procédures ;
- nous conformer aux prescriptions législatives et réglementaires et aux normes, et les dépasser lorsque c'est possible ;
- veiller à ce que des ressources humaines suffisamment compétentes et entraînées soient disponibles pour mettre en œuvre les stratégies et processus de sécurité ;
- veiller à ce que tout le personnel reçoive une information et une formation adéquates et appropriées relatives à la sécurité de l'aviation, soit compétent sur les questions de sécurité, et que seules des tâches correspondant à ses compétences lui soient attribuées ;
- établir et mesurer notre performance de sécurité par rapport à des indicateurs et cibles réalistes de performance de sécurité ;
- améliorer constamment notre performance de sécurité grâce à une surveillance et une évaluation continues, à des examens et ajustements périodiques des objectifs et cibles en matière de sécurité et à la réalisation rapide de ces objectifs et cibles ;
- s'assurer que les systèmes et services de sécurité fournis de l'extérieur pour appuyer nos opérations répondent à nos normes de performance de sécurité.

(Signé) _____
Directeur général/Administrateur gérant/ou titre approprié

Figure 5-1. Exemple d'énoncé de politique de sécurité

- c) de se conformer aux normes internationales ;
- d) d'adopter des meilleures pratiques éprouvées, convenant à l'activité ;
- e) de fournir toutes les ressources nécessaires ;
- f) de veiller à ce que la sécurité soit une responsabilité principale de tous les gestionnaires ;
- g) de suivre la politique disciplinaire ;
- h) de veiller à ce que la politique de sécurité soit comprise, mise en œuvre et maintenue à tous les niveaux.

5.3.13 Les normes de sécurité obtenues sont une indication du comportement de l'organisation et sont également une mesure de la performance du SGS. En outre, les objectifs de sécurité et les normes de performance de sécurité doivent être liés :

- a) aux indicateurs de performance de sécurité ;
- b) aux cibles de performance de sécurité ;
- c) aux actions d'atténuation du SGS.

5.3.14 La politique disciplinaire sert à déterminer si une violation qui s'est produite exige des mesures allant au-delà des besoins de l'analyse des systèmes de gestion des risques. Il est donc essentiel de s'assurer que les personnes responsables de faire cette détermination ont la compétence technique nécessaire pour prendre pleinement en compte le contexte lié au rapport, ce qui diminuera la probabilité que ces personnes et le prestataire de services lui-même soit exposé à des procédures « disciplinaires/judiciaires » injustes ou inappropriées. Une méthode qui peut être utilisée pour prendre cette décision est l'algorithme des actes dangereux de James Reason pour aider les gestionnaires de première ligne à déterminer l'imputabilité des personnes ayant été impliquées dans un incident¹. Un autre ouvrage utile également à cet égard est le livre de Sidney Dekker intitulé *Just Culture : Balancing Safety and Accountability*².

5.3.15 Une politique appropriée de protection des données de sécurité et des sources qui communiquent ces données, peut avoir un effet positif important sur la culture de compte rendu. Une fois qu'il est clair qu'un compte rendu ne comprend pas une violation, le prestataire de services et l'État devraient permettre la dépersonnalisation et l'agrégation des comptes rendus de façon à mener une analyse de sécurité utile sans impliquer le personnel ou un prestataire de services spécifique. Parce que de grands événements peuvent invoquer des processus et procédures qui sortent du cadre du SGS du prestataire de services, l'autorité compétente de l'État peut ne pas permettre la dépersonnalisation rapide des comptes rendus dans tous les cas. Néanmoins, une politique permettant la dépersonnalisation appropriée des comptes rendus peut nettement améliorer la qualité des données recueillies.

1. James Reason, *Managing the Risks of Organisational Accidents*, 1997.

2. Sidney Dekker, *Just Culture: Balancing Safety and Accountability*, Second Edition, 2012.

Élément 1.2 du SGS Obligations de rendre compte en matière de sécurité

Le prestataire de services devra :

- a) désigner le Dirigeant responsable qui, indépendamment d'autres fonctions, aura la responsabilité et l'imputabilité ultimes, au nom de [l'organisation], de la mise en œuvre et de la maintenance du SGS ;
- b) définir clairement l'imputabilité hiérarchique en matière de sécurité dans l'ensemble de l'organisation y compris l'imputabilité directe des cadres supérieurs en matière de sécurité ;
- c) préciser les obligations redditionnelles de tous les membres de la direction, indépendamment d'autres fonctions, ainsi que celles des employés, en ce qui concerne la performance de sécurité du SGS ;
- d) documenter et communiquer dans toute l'organisation les responsabilités, imputabilités et les pouvoirs en matière de sécurité ;
- e) définir les niveaux de direction qui sont habilités à prendre des décisions en ce qui concerne la tolérabilité des risques de sécurité.

Orientations générales

5.3.16 Dans le contexte du SGS, l'imputabilité signifie le fait d'être ultimement responsable de la performance de sécurité, que ce soit au niveau global du SGS (Dirigeant responsable) ou aux niveaux de produits/processus spécifiques (membres de l'équipe de gestion). Cela comprend la responsabilité de veiller à ce que des actions correctrices appropriées soient prises pour contrer les dangers et remédier aux erreurs dont il a été rendu compte, ainsi que de réagir à des accidents et incidents.

5.3.17 Historiquement, dans la plupart des organisations, le bureau de la sécurité gérait l'ensemble du processus de sécurité au sein de l'organisation. Ce fonctionnaire de la sécurité était la personne à qui il revenait d'identifier les questions de sécurité, de proposer des solutions, de participer à la mise en œuvre des solutions et de suivre l'efficacité des solutions. Cette pratique attribuait totalement le processus de sécurité au bureau de la sécurité, éliminant ainsi du processus de décision en matière de sécurité les dirigeants et les gestionnaires de première ligne. Cela donnait l'impression que les questions de sécurité sortaient de la responsabilité du gestionnaire de première ligne ; les problèmes de sécurité étaient considérés comme étant de la responsabilité du bureau de la sécurité et du fonctionnaire chargé de la sécurité. En outre, cette approche ignorait la contribution précieuse que pouvaient apporter les unités de production et les unités opérationnelles au processus décisionnel de l'organisation en matière de sécurité.

5.3.18 En exigeant du prestataire de services qu'il désigne le Dirigeant responsable, la responsabilité de la performance globale de sécurité est placée à un niveau de l'organisation qui a l'autorité pour prendre des décisions et veiller à ce que le SGS soit efficace. Le fait de définir les obligations redditionnelles spécifiques en matière de sécurité de tous les membres de l'équipe de direction précise clairement le cadre d'imputabilité dans toute l'organisation. Ce cadre d'imputabilité doit comprendre l'obligation de rendre compte de la performance de sécurité du sous-produit ou des prestataires de services travaillant en sous-traitance et qui n'exigent pas séparément une certification ou une approbation de sécurité. Ces responsabilités, imputabilités et pouvoirs en matière de sécurité doivent être documentés et communiqués à toute l'organisation et ils doivent préciser les niveaux de gestion qui sont habilités à prendre des décisions en ce qui concerne la tolérabilité des risques de sécurité. En outre, les imputabilités des gestionnaires en

matière de sécurité devraient comprendre l'attribution des ressources humaines, techniques, financières et autres ressources pour une performance efficace et efficiente du SGS.

Note.— Dans le contexte du SGS, le terme « imputabilités » peut s'entendre de responsabilités qui ne devraient pas être déléguées.

Stratégie de mise en œuvre

5.3.19 Pour tout prestataire de services d'aviation, la gestion de la sécurité devrait être une fonction essentielle. La définition des imputabilités pour tout le personnel remplissant des fonctions de sécurité serviront à garantir la fourniture de produits et opérations sûrs, ainsi qu'une répartition convenablement équilibrée des ressources.

5.3.20 Le Dirigeant responsable désigné par le prestataire de services est l'unique personne ayant la responsabilité ultime du SGS, y compris la responsabilité de fournir les ressources essentielles à sa mise en œuvre et à sa maintenance. Les pouvoirs et responsabilités du Dirigeant responsable comprennent, mais sans s'y limiter :

- a) la fourniture et la répartition des ressources humaines, techniques, financières ou autres ressources nécessaires à la performance efficace et efficiente du SGS ;
- b) la responsabilité directe de la conduite des affaires de l'organisation ;
- c) l'autorité finale sur les opérations conduites en vertu du certificat/approbation de l'organisation ;
- d) l'établissement et la promotion de la politique de sécurité ;
- e) la détermination des objectifs de sécurité et des cibles de sécurité de l'organisation ;
- f) le rôle de champion de la sécurité de l'organisation ;
- g) la responsabilité finale de la résolution de toutes les questions de sécurité ;
- h) l'établissement et le maintien de l'aptitude de l'organisation à tirer les leçons de l'analyse des données recueillies dans le cadre de son système de comptes rendus de sécurité.

Note.— Les responsabilités décrites ci-dessus ne devraient pas être déléguées.

5.3.21 Selon la taille, la structure et la complexité de l'organisation, le Dirigeant responsable peut être :

- a) le directeur général (CEO) de l'organisation du prestataire de services;
- b) le président du conseil d'administration ;
- c) un associé ;
- d) le propriétaire.

5.3.22 En outre, la nomination d'un Dirigeant responsable auquel sont attribués les pouvoirs et responsabilités nécessaires commande que cette personne ait les qualifications nécessaires pour s'acquitter du rôle. Le Dirigeant responsable aura de nombreuses fonctions dans l'organisation. Néanmoins, le rôle du Dirigeant responsable est d'installer la sécurité comme valeur essentielle de l'organisation et de veiller à ce que le SGS soit correctement mis en œuvre et préservé au moyen de l'attribution des ressources et des tâches.

5.3.23 Tous les postes, toutes les responsabilités et tous les pouvoirs en matière de sécurité de l'aviation devraient être définis, documentés et communiqués dans l'ensemble de l'organisation. Les imputabilités de chaque haut dirigeant en matière de sécurité (chef de service ou personne chargée d'une unité fonctionnelle) sont des composantes intégrales de leur description de poste. La gestion de la sécurité étant une fonction d'entreprise essentielle, chaque gestionnaire supérieur sera impliqué à un degré divers dans le fonctionnement du SGS. Cette implication sera certainement plus approfondie pour les gestionnaires responsables d'unités fonctionnelles fournissant les produits ou services de l'organisation (opérations, fabrication, maintenance, ingénierie, formation et *affectation*, désignés ci-après sous le terme générique « cadres hiérarchiques ») que pour ceux qui sont responsables de fonctions de soutien (ressources humaines, administration, services juridiques et financiers).

5.3.24 Le prestataire de services est responsable de la performance de sécurité des services ou des produits fournis par des sous-traitants pour lesquels une certification ou approbation de sécurité séparée n'est pas requise. Tous les sous-contractants ne sont peut-être pas nécessairement tenus d'avoir un SGS, mais il est néanmoins de la responsabilité du prestataire de services de s'assurer que ses propres exigences en matière de performance de sécurité sont satisfaites. De toute façon, il est essentiel que le SGS du prestataire de services fonctionne aussi harmonieusement que possible avec les systèmes de sécurité des sous-traitants qui fournissent les produits ou services pertinents à la sécurité de l'exploitation des aéronefs. L'interface entre le SGS de l'organisation avec celui des systèmes de sécurité du sous-prestataire de produits ou de services doit prendre en compte l'identification des dangers, l'évaluation des risques et l'élaboration de stratégies d'atténuation des risques, le cas échéant. Le prestataire de services devrait veiller :

- a) à ce qu'il y ait une politique établissant clairement un schéma des imputabilités et de l'autorité en matière de sécurité entre le prestataire de services et le sous-traitant ;
- b) à ce que le sous-traitant ait un système de compte rendu de sécurité à la mesure de sa taille et de sa complexité, qui facilite l'identification précoce des dangers et les défaillances systémiques qui concernent le prestataire de services ;
- c) à ce que le comité d'examen de la sécurité du prestataire de services comprenne un représentant du sous-traitant, selon le cas ;
- d) à ce que soient élaborés, selon le cas, des indicateurs de sécurité/qualité pour suivre la performance du sous-traitant ;
- e) à ce que le processus de promotion de la sécurité du prestataire de services garantisse que les employés du sous-traitant reçoivent les communications de sécurité applicables de l'organisation ;
- f) à ce que les rôles, responsabilités et fonctions de tout sous-traitant qui soient pertinents au Plan d'intervention d'urgence du prestataire de services soient élaborés et testés.

5.3.25 Les imputabilités, responsabilités et pouvoirs de tous les gestionnaires supérieurs compétents, dans le cadre du SGS, doivent être décrits dans la documentation relative au SGS de l'organisation. Des fonctions de sécurité obligatoires accomplies par le directeur de la sécurité, le bureau de la sécurité, les groupes d'action pour la sécurité, etc., peuvent être intégrées dans les descriptions de poste, processus et procédures existants.

5.3.26 La fonction du directeur de la sécurité est décrite en détail dans la section suivante. S'agissant de l'imputabilité, la personne qui occupe la fonction de directeur de la sécurité est responsable devant le Dirigeant responsable de la performance du SGS et de la fourniture des services de sécurité aux autres services de l'organisation.

Élément 1.3 du SGS Nomination du personnel clé de sécurité

Le prestataire de services nommera un directeur de la sécurité responsable de la mise en œuvre et de la maintenance d'un SGS efficace.

Orientations générales

5.3.27 La nomination d'un directeur de la sécurité qualifié est essentielle à la mise en œuvre et au fonctionnement efficaces d'un bureau des services de sécurité. Cette personne sera désignée par des titres divers dans différentes organisations, mais aux fins du présent manuel le terme générique directeur de la sécurité est utilisé.

Stratégie de mise en œuvre

5.3.28 Le directeur de la sécurité, dans la plupart des organisations, est la personne responsable du développement et de la maintenance d'un SGS efficace. Le directeur de la sécurité conseille aussi le Dirigeant responsable et les cadres hiérarchiques sur les questions relatives à la gestion de la sécurité et est chargé de coordonner les questions de sécurité et de communiquer à leur sujet au sein de l'organisation, ainsi qu'avec les agences, sous-traitants et parties prenantes de l'extérieur. Les fonctions du directeur de la sécurité consistent, sans nécessairement s'y limiter, à :

- a) gérer le plan de mise en œuvre du SGS au nom du Dirigeant responsable ;
- b) exécuter/faciliter l'identification des dangers et l'analyse des risques de sécurité ;
- c) surveiller les mesures correctives et évaluer leurs résultats ;
- d) présenter des rapports périodiques sur la performance de sécurité de l'organisation ;
- e) tenir les dossiers et la documentation relative à la sécurité ;
- f) planifier et organiser la formation du personnel en matière de sécurité ;
- g) donner des avis indépendants sur les questions de sécurité ;
- h) surveiller les préoccupations de sécurité dans l'industrie de l'aviation et leurs effets ressentis sur les opérations de l'organisation axées sur la fourniture de services ;
- i) coordonner et communiquer (au nom du Dirigeant responsable) avec l'autorité nationale de supervision et les autres agences de l'État, selon les besoins, au sujet des questions relatives à la sécurité ;
- j) coordonner et communiquer (au nom du Dirigeant responsable) avec les agences internationales au sujet des questions relatives à la sécurité.

5.3.29 Les critères de sélection d'un directeur de la sécurité devraient comprendre, mais sans s'y limiter, les qualifications suivantes :

- a) expérience de la gestion de la sécurité/qualité ;

- b) expérience opérationnelle ;
- c) bagage technique pour comprendre les systèmes qui appuient les opérations ;
- d) compétences humaines ;
- e) compétences analytiques et de résolution de problèmes ;
- f) compétences en gestion de projets ;
- g) compétences en communication orale et écrite.

Note.— Une description de poste type pour un directeur de la sécurité figure à l'Appendice 2 au présent chapitre. Pour les petits organismes, il peut être viable de combiner les fonctions de gestion de la sécurité et de la qualité au sein du même bureau.

5.3.30 Le directeur de la sécurité est généralement appuyé par du personnel supplémentaire. Cela dépendra de la taille de l'organisation ainsi que de sa nature et de sa complexité. Le directeur de la sécurité assure directement la liaison avec les cadres hiérarchiques ou leurs délégués, par exemple lorsque des unités opérationnelles sont appuyées par des agents de sécurité dédiés.

5.3.31 Le directeur de la sécurité est responsable de la collecte et de l'analyse des données de sécurité ainsi que de la diffusion des renseignements connexes sur la sécurité aux cadres hiérarchiques. La diffusion par le bureau des services de sécurité des renseignements sur les risques de sécurité est la première étape du processus de gestion de ces risques. Cette information doit être utilisée par les cadres hiérarchiques pour atténuer les risques de sécurité, ce qui inévitablement exige l'affectation de ressources. Les ressources nécessaires peuvent être facilement mises à la disposition des cadres hiérarchiques à cet effet.

5.3.32 En outre, il faut un processus formel pour évaluer l'efficacité et l'efficience des stratégies d'atténuation utilisées pour atteindre les cibles de performance de sécurité convenues de l'organisation. Un processus possible inclut la création d'un comité d'examen de la sécurité (SRC). Le comité d'examen de la sécurité (SRC) fournit la plate-forme pour réaliser les objectifs d'attribution de ressources et évaluer l'efficacité et l'efficience des stratégies d'atténuation des risques. Le SRC est un comité de très haut niveau, présidé par le Dirigeant responsable et composé de cadres supérieurs, y compris les cadres hiérarchiques responsables des domaines fonctionnels et ceux des services administratifs pertinents. Le directeur de la sécurité participe au SRC, avec voix consultative uniquement. Le SRC peut ne pas se réunir souvent, à moins que des circonstances exceptionnelles n'exigent qu'il en soit autrement. Le SRC :

- a) surveille l'efficacité du SGS ;
- b) veille à ce que toutes mesures correctives nécessaires soient prises en temps voulu ;
- c) surveille la performance de sécurité par rapport à la politique et aux objectifs de sécurité de l'organisation ;
- d) surveille l'efficacité des processus de gestion de la sécurité de l'organisation qui appuient sa priorité déclarée de gestion de la sécurité comme un des processus d'entreprise essentiels ;
- e) surveille l'efficacité de la supervision de la sécurité des opérations sous-traitées ;
- f) veille à ce que les ressources appropriées soient attribuées pour réaliser une performance de sécurité dépassant celle qu'exige le respect des règlements ;

5.3.33 Le SRC est stratégique et traite de questions de haut niveau en relation avec les politiques, l'attribution de ressources et la surveillance de la performance organisationnelle. Une fois l'orientation stratégique mise au point par le SRC, la mise en œuvre des stratégies de sécurité doit être coordonnée à l'échelle de l'organisation toute entière. Cela peut se faire par la création de Groupes d'action pour la sécurité (GAS), qui se composent de cadres hiérarchiques et d'agents de première ligne et sont généralement présidés par un cadre hiérarchique désigné. Les SAG sont des entités tactiques qui traitent de questions de mise en œuvre spécifiques sous la direction du SRC. Le SRC :

- a) supervise la performance de sécurité opérationnelle dans les domaines fonctionnels de l'organisation et veille à ce que des activités appropriées de gestion des risques de sécurité soient menées avec la participation du personnel nécessaire à un renforcement de la prise de conscience en matière de sécurité ;
- b) coordonne la résolution de stratégies d'atténuation pour les conséquences identifiées de dangers et s'assure de l'existence d'arrangements satisfaisants pour la capture des données de sécurité et les retours d'information des employés ;
- c) évalue l'impact que des changements opérationnels ou nouvelles technologies pourraient avoir sur la sécurité ;
- d) coordonne la mise en œuvre de plans d'action correctrice et veille à ce que les mesures correctrices soient prises en temps voulu ;
- e) examine l'efficacité des recommandations de sécurité antérieures ;
- f) supervise la promotion de la sécurité en tant que de besoin pour sensibiliser davantage les employés aux questions de sécurité et veiller à ce qu'il leur soit offert des possibilités appropriées de participer à des activités de gestion de la sécurité.

Élément 1.4 du SGS Coordination de la planification des interventions d'urgence

Le prestataire de services veille à ce qu'un plan d'intervention d'urgence soit dûment coordonné avec les plans d'intervention d'urgence des organisations avec lesquelles il doit entrer en interface pendant la fourniture de ses services.

Stratégie de mise en œuvre

5.3.34 Le Plan d'intervention d'urgence (ERP) énonce les mesures qui doivent être prises par tout le personnel responsable en cas de situation d'urgence liée à l'aviation. L'objet d'un ERP est d'assurer une transition ordonnée et efficace des opérations normales aux opérations d'urgence, y compris l'attribution des responsabilités d'urgence et la délégation de pouvoirs pour les situations d'urgence. L'autorisation des mesures à prendre par le personnel clé figure aussi dans le plan, ainsi que les moyens de la coordination des efforts nécessaires pour faire face à l'urgence. L'objectif général est de sauver des vies, de poursuivre les opérations en sécurité et de retourner dès que possible à des opérations normales.

5.3.35 L'applicabilité de la planification des interventions d'urgence s'étend aux fournisseurs de produits d'aviation qui peuvent être attribuables à un événement lié à la sécurité de l'aviation ou touchés par cet événement. Les processus du prestataire du produit sont généralement appelés « soutien technique d'urgence » et comprennent des mesures de navigabilité d'urgence, des services d'alerte et du soutien sur le lieu d'un accident d'aviation. Le fournisseur

du produit n'a pas besoin de changer le nom de ces processus de soutien technique au produit en les désignant « processus ERP » ; toutefois, ces processus de soutien technique doivent être notés de manière appropriée dans les documents relatifs au SGS de l'organisation. Voir l'Appendice 3 pour d'autres orientations sur l'ERP.

Élément 1.5 du SGS Documentation relative au SGS

1.5.1 Le prestataire de services élabore un plan de mise en œuvre du SGS, formellement entériné par l'organisation, qui définit la démarche de celle-ci en matière de gestion de la sécurité d'une manière répondant à ses objectifs de sécurité.

1.5.2 Le prestataire de services élabore et tient à jour la documentation du SGS, qui décrira :

- a) la politique et les objectifs de sécurité ;
- b) les exigences du SGS ;
- c) les processus et procédures du SGS ;
- d) les imputabilités, responsabilités et pouvoirs pour les processus et procédures du SGS ;
- e) les produits du SGS.

1.5.3 Dans le cadre de la documentation relative au SGS, le prestataire de services développe et tient à jour un manuel SGS.

Orientations générales

5.3.36 La documentation du SGS devrait comprendre un document de description du plus haut niveau (exposition), qui décrit le SGS de l'organisation selon ses composants et éléments. Ce document facilite l'administration, la communication et la tenue à jour du SGS au sein de l'organisation. En même temps, il sert de communication du SGS de l'organisation (déclaration) à l'autorité compétente (AAC) aux fins de l'acceptation, de l'évaluation et de la supervision réglementaires ultérieures du SGS. Ce document SGS de haut niveau peut être un document séparé ou peut être une « section/chapitre du SGS » dans un document existant de l'organisation ou approuvé par l'AAC. Lorsque des détails des processus SGS de l'organisation sont déjà traités dans des documents existants, des renvois appropriés à ces documents suffisent. Ce document SGS devra être tenu à jour et, lorsque des amendements significatifs sont prévus ou y sont apportés, ils peuvent nécessiter l'accord de l'AAC, selon le cas. Des orientations sur la compilation d'un document SGS figurent dans l'Appendice 4.

5.3.37 Un autre aspect de la documentation relative au SGS est la compilation et la tenue à jour de dossiers qui attestent de l'existence et du fonctionnement continu du SGS. Ces dossiers devraient être organisés selon les éléments et processus associés respectifs du SGS. Pour certains processus il peut être suffisant que le système de documentation du SGS comprenne des copies ou des échantillons de dossiers tenus dans le cadre d'autres systèmes de documentation de l'organisation (par exemple le département des dossiers techniques et la bibliothèque centrale). Lors de la phase de mise en œuvre initiale, la documentation relative au SGS peut comprendre un dossier sur l'analyse des écarts et le plan de mise en œuvre progressive.

Stratégie de mise en œuvre

5.3.38 La documentation relative au SGS couvre tous les éléments et processus du SGS et comprend normalement :

- a) une description récapitulative des composants et éléments du SGS, comme :
 - 1) la gestion des documents et des dossiers,
 - 2) les exigences réglementaires du SGS,
 - 3) le cadre, la portée et l'intégration,
 - 4) la politique et les objectifs de sécurité,
 - 5) les imputabilités en matière de sécurité et le personnel clé correspondant,
 - 6) le système de comptes rendus volontaires de dangers,
 - 7) les procédures de comptes rendus d'incidents et d'enquêtes,
 - 8) les processus d'identification des dangers et d'évaluation des risques,
 - 9) les indicateurs de performance de sécurité,
 - 10) la formation et la communication en matière de sécurité,
 - 11) l'amélioration continue et l'audit du SGS,
 - 12) la gestion du changement,
 - 13) la planification des interventions d'urgence ou opérations d'urgence ;
- b) une compilation des dossiers et documents actuels concernant le SGS, par exemple :
 - 1) le registre des comptes rendus de dangers et des échantillons de rapports réels,
 - 2) les indicateurs de performance de sécurité et les graphiques connexes,
 - 3) le dossier des évaluations de sécurité achevées ou en cours,
 - 4) les dossiers des examens ou audits internes du SGS,
 - 5) les dossiers de la promotion de la sécurité,
 - 6) les dossiers de la formation du personnel au SGS/sécurité,
 - 7) les procès-verbaux des réunions du comité de la sécurité du SGS,
 - 8) le plan de mise en œuvre du SGS (pendant le processus de mise en œuvre).

Composant 2 du SGS. Gestion des risques de sécurité*Orientations générales*

5.3.39 Les prestataires de services devraient veiller à ce que les risques de sécurité rencontrés dans les activités d'aviation soient maîtrisés afin de réaliser leurs cibles de performance de sécurité. Ce processus est connu sous l'appellation « gestion des risques de sécurité » et comprend l'identification des dangers, l'évaluation des risques de sécurité et la mise en œuvre de mesures correctrices appropriées. Le processus de gestion des risques de sécurité est illustré à la Figure 5-2.

5.3.40 Le composant gestion des risques de sécurité identifie systématiquement les dangers qui existent dans le contexte de la fourniture de ses produits ou services. Les dangers peuvent résulter de systèmes qui sont défectueux au niveau de la conception, de la fonction technique, de l'interface humaine ou des interactions humaines avec d'autres processus et systèmes. Ils peuvent également résulter d'un échec de processus ou systèmes existants à s'adapter aux changements de l'environnement opérationnel du prestataire de services. Une analyse soignée de ces facteurs pendant les phases de planification, de conception et de mise en œuvre peut souvent aider à déterminer les dangers potentiels avant que le système devienne opérationnel.

5.3.41 La compréhension du système et de son environnement opérationnel est également essentielle pour la réalisation de performances de sécurité élevées. Les dangers peuvent être découverts pendant le cycle de vie opérationnel, grâce aux comptes rendus des employés ou aux enquêtes sur les incidents. L'analyse de ces dangers devrait être menée dans le contexte du système. Ce contexte est essentiel si l'on veut éviter l'attribution d'événements à l'« erreur humaine », auquel cas des défauts du système peuvent être négligés, qui restent cachés et susceptibles de jouer un rôle dans des événements futurs potentiellement plus graves. Des orientations sur les procédures d'identification des dangers et d'évaluation des risques et sur leur présentation sont traitées dans les paragraphes 5.3.42 à 5.3.61 ainsi que dans le Chapitre 2, paragraphes 2.14 et 2.15, respectivement.

Élément 2.1 du SGS Identification des dangers

2.1.1 Le prestataire de services élabore et tient à jour un processus formel qui assure l'identification des dangers des produits ou services associés à l'aviation.

2.1.2 L'identification des dangers se fonde sur une combinaison de méthodes réactives, proactives et prédictives de collecte de données de sécurité.

Orientations générales

5.3.42 La gestion des risques de sécurité commande que le prestataire de services élabore et maintienne un processus formel pour identifier les dangers qui pourraient contribuer à des événements liés à la sécurité de l'aviation. Des dangers peuvent exister dans les activités permanentes de l'aviation ou être introduits par inadvertance dans une opération chaque fois que des changements sont introduits dans le système d'aviation. Dans ce cas, l'identification des dangers fait partie intégrante des processus de gestion du changement comme il est décrit dans l'élément 3.2 du SGS — La gestion du changement.

5.3.43 L'identification des dangers est basée sur une combinaison de méthodes réactives, proactives et prédictives de collecte des données sur la sécurité, comme il a été vu au Chapitre 2. L'identification des dangers est la première étape du processus de gestion des risques de sécurité. Les risques de sécurité correspondants sont alors évalués dans le contexte des conséquences potentiellement dommageables liées au danger. Lorsque les risques de sécurité sont jugés inacceptables, d'autres contrôles des risques de sécurité doivent être intégrés dans le système.

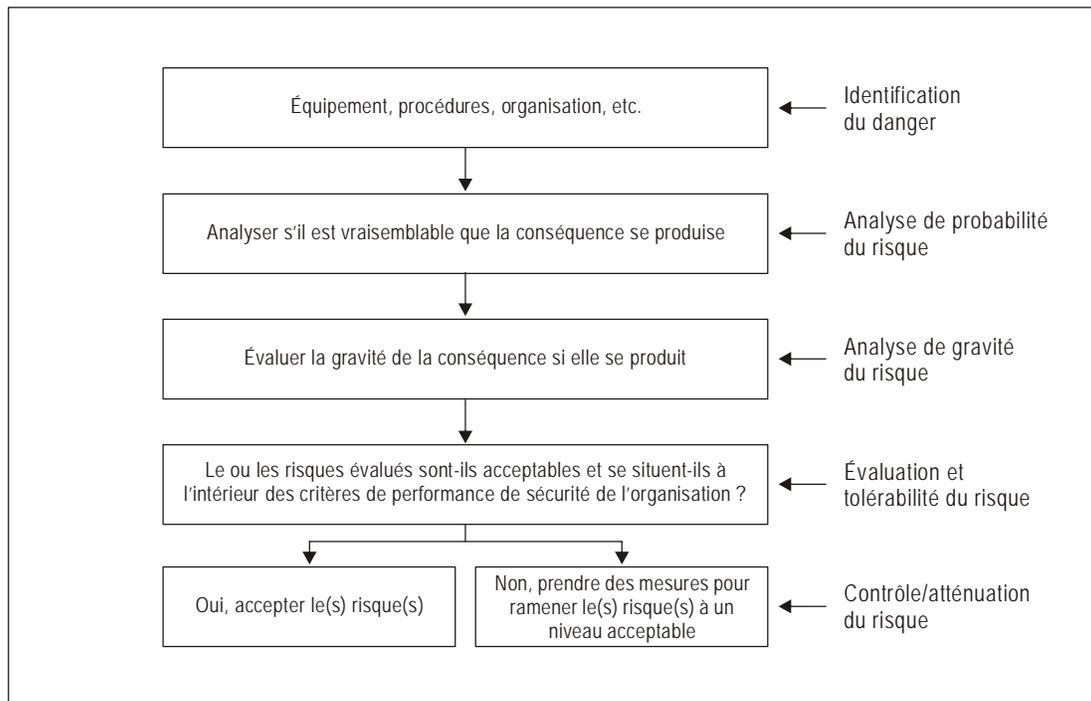


Figure 5-2. Processus de gestion des risques de sécurité

5.3.44 Dans les systèmes de gestion de la sécurité bien au point, l'identification des dangers est continue et fait partie intégrante des processus organisationnels du prestataire de services. Plusieurs conditions déclenchent des activités plus approfondies et plus étendues d'identification des dangers et peuvent comprendre :

- a) les cas où l'organisation connaît une augmentation inexplicquée d'événements liés à la sécurité de l'aviation ou de non-respect des règlements en matière de sécurité de l'aviation ;
- b) d'importants changements opérationnels, y compris des changements prévus du personnel clé ou d'autres composants majeurs du système ;
- c) d'importants changements organisationnels, y compris la croissance et la contraction prévues, des fusions d'entreprises ou des acquisitions.

5.3.45 Une approche structurée de l'identification des dangers peut comprendre l'utilisation de sessions de remue-méninges en groupe, au cours desquelles des experts spécialistes procèdent à des scénarios d'analyse détaillés. Les sessions d'identification des dangers exigent toute une gamme de personnel opérationnel et technique expérimenté et sont gérées par un facilitateur. Le même groupe peut également être utilisé pour évaluer les risques de sécurité correspondants.

5.3.46 Le système de gestion de l'information de sécurité du prestataire de services devrait comprendre des documents relatifs à l'évaluation de la sécurité, contenant des descriptions des dangers, les conséquences connexes, la probabilité et la gravité estimées des risques de sécurité et les contrôles des risques de sécurité requis. Les évaluations de sécurité existantes devraient être examinées toutes les fois que de nouveaux dangers sont détectés et que l'on prévoit d'autres propositions de contrôle des risques de sécurité.

5.3.47 La Figure 5-3 illustre le processus de documentation des dangers et de la gestion des risques qui s'ensuit. Les dangers sont constamment identifiés grâce à diverses sources de données. On attend du prestataire de services qu'il identifie les dangers, les élimine ou atténue les risques associés. Dans le cas de dangers identifiés dans des produits ou services fournis par l'intermédiaire de sous-traitants, une atténuation pourrait être l'exigence, de la part du prestataire de services, que ces organisations aient un SGS ou un processus équivalent d'identification des dangers et de gestion des risques.

5.3.48 Le système d'information sur la gestion de la sécurité devient une source de connaissances sur la sécurité à utiliser comme référence pour les prises de décisions organisationnelles intéressant la sécurité. Ces connaissances en matière de sécurité constituent des éléments pour les analyses de tendances en matière de sécurité, ainsi qu'à des fins d'éducation en matière de sécurité. Des orientations sur les systèmes de comptes rendus volontaires et confidentiels de dangers sont présentées dans l'Appendice 5.

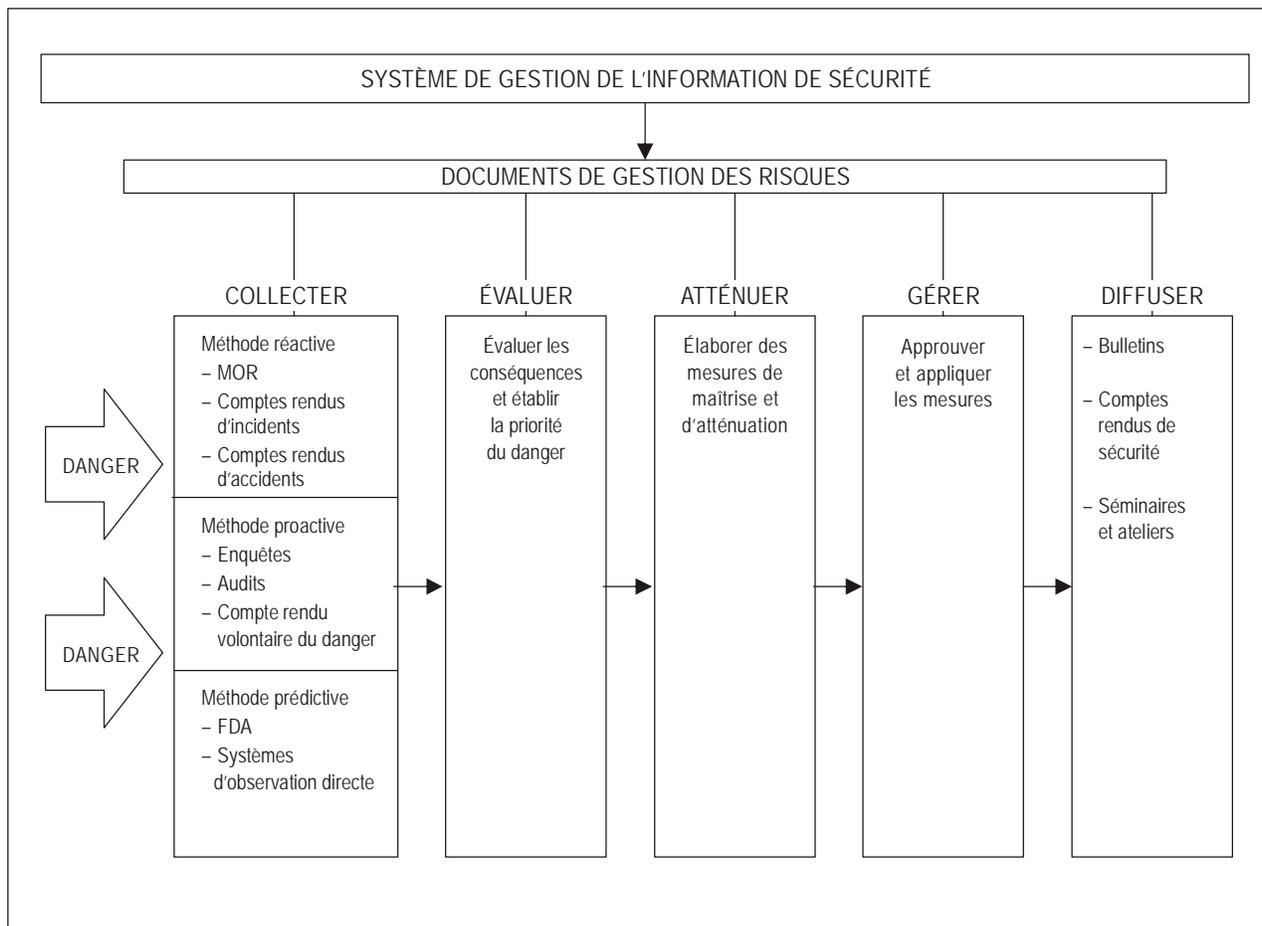


Figure 5-3. Documentation des dangers et le processus de gestion des risques qui s'ensuit

Stratégie de mise en œuvre

5.3.49 Dans le cadre du processus d'identification des dangers, les éléments ci-après peuvent être examinés :

- a) les facteurs de conception, y compris la conception de l'équipement et des tâches ;
- b) les limites des performances humaines (par exemples limites physiologiques, psychologiques et cognitives) ;
- c) les procédures et pratiques d'exploitation, y compris la documentation et les listes de vérification s'y rapportant, et leur validation en conditions d'exploitation réelles ;
- d) les facteurs de la communication, y compris les médias, la terminologie et la langue ;
- e) les facteurs organisationnels, tels que ceux qui sont liés au recrutement, à la formation et à la rétention du personnel, la compatibilité des objectifs de production et de sécurité, l'affectation des ressources, les pressions de l'exploitation, et la culture de sécurité de l'entreprise ;
- f) les facteurs de milieu de travail (par exemple le bruit ambiant et les vibrations, la température, l'éclairage et la disponibilité de vêtements et d'équipement de protection) ;
- g) les facteurs de supervision réglementaire, incluant l'applicabilité des règlements et leur force exécutoire, la certification de l'équipement, du personnel et des procédures ;
- h) les systèmes de surveillance des performances qui peuvent détecter la dérive pratique ou les écarts opérationnels ;
- i) les facteurs concernant l'interface humain-machine.

5.3.50 Les dangers peuvent être identifiés à travers des processus proactifs et prédictifs ou à la suite d'enquêtes sur un accident ou un incident. Il existe diverses sources d'identification des dangers ; certaines sources sont intérieures à l'organisation, tandis que d'autres lui sont extérieures. Voici des exemples de sources internes d'identification des dangers :

- a) dispositifs de surveillance des opérations normales (par exemple l'analyse des données de vol pour les exploitants d'aéronefs) ;
- b) système de comptes rendus volontaires et obligatoires ;
- c) études sur la sécurité ;
- d) audits de sécurité ;
- e) retour d'information provenant de la formation ;
- f) rapports sur les enquêtes sur accidents/incidents et leur suivi.

5.3.51 Exemples de sources externes pour identifier les dangers :

- a) rapports d'accidents de l'industrie ;
- b) systèmes nationaux de comptes rendus obligatoires d'événements ;
- c) systèmes nationaux de comptes rendus volontaires d'événements ;

- d) audits de supervision nationaux ;
- e) systèmes d'échange d'information.

5.3.52 Le type de technologies utilisées dans le processus d'identification des dangers dépendra de la taille et de la complexité du prestataire de services et de ses activités d'aviation. Dans tous les cas, le processus d'identification des dangers du prestataire de services est clairement décrit dans les documents relatifs au SGS/sécurité de l'organisation. Le processus d'identification des dangers analyse tous les dangers possibles qui peuvent exister dans le cadre des activités d'aviation du prestataire de services, y compris les interfaces avec d'autres systèmes, aussi bien à l'intérieur qu'à l'extérieur de l'organisation. Une fois les dangers identifiés, leurs conséquences (c'est-à-dire tous événements ou résultats spécifiques) devraient être déterminées. Voir l'Appendice 5 pour des orientations sur le système de comptes rendus volontaires et confidentiels d'une organisation.

Élément 2.2 du SGS Évaluation et atténuation des risques de sécurité

Le prestataire de services élabore et tient à jour un processus qui garantit l'analyse, l'évaluation et la maîtrise des risques de sécurité associés aux dangers identifiés.

Orientations générales

5.3.53 La Figure 5-4 présente l'ensemble du processus de gestion des risques de sécurité. Ce processus commence par l'identification des dangers et de leurs conséquences potentielles. Les risques de sécurité sont alors évalués en termes de probabilité et de gravité afin de définir le niveau du risque de sécurité (indice de risque de sécurité). Si les risques de sécurité sont jugés tolérables, les mesures jugées appropriées sont prises et l'opération se poursuit. Une fois achevé, le processus d'identification des dangers et d'évaluation des risques de sécurité et d'atténuation est documenté et approuvé, selon le cas, et fait partie du système de gestion de l'information de sécurité.

5.3.54 Si les risques de sécurité sont jugés inacceptables, les questions suivantes deviennent pertinentes :

- a) *Est-il possible d'éliminer les dangers et les risques de sécurité associés ?* Si la réponse est oui, alors les mesures appropriées sont prises et documentées. Si la réponse est non, la question suivante est :
- b) *Est-il possible d'atténuer le ou les risques de sécurité ?* Si la réponse est non, les activités connexes doivent être annulées. Si la réponse est oui, des mesures d'atténuation appropriées sont prises et la question suivante est :
- c) *Existe-t-il des risques résiduels de sécurité quelconques ?* Si la réponse est oui, alors les risques résiduels doivent être évalués afin de déterminer leur niveau de tolérabilité et de savoir également s'ils peuvent être éliminés ou atténués selon les besoins afin de garantir un niveau acceptable de performance de sécurité.

5.3.55 L'évaluation des risques de sécurité comprend une analyse des dangers identifiés, qui comprend deux composants :

- a) la gravité du résultat de sécurité ;
- b) la probabilité que ce résultat surviendra.

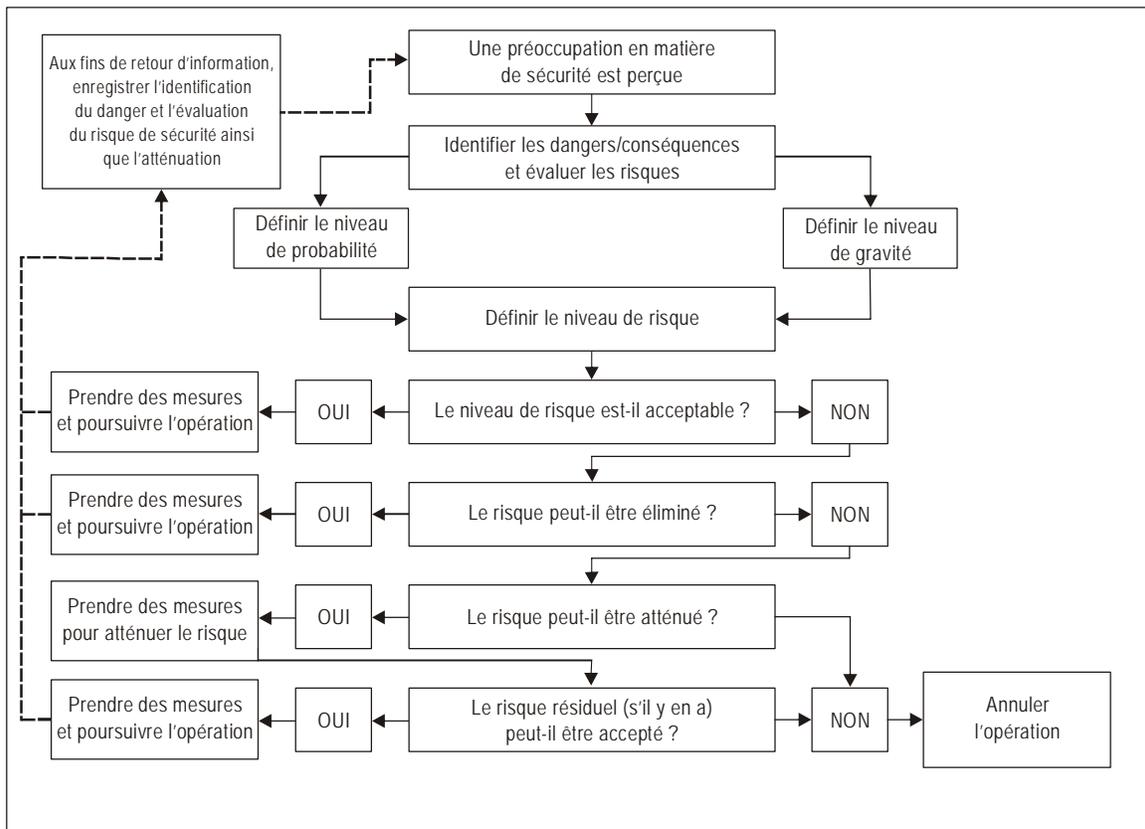


Figure 5-4. Le processus de gestion des risques de sécurité

Des orientations sur la façon dont l'information de sécurité devrait être analysée dans les organisations complexes et vastes figurent au Chapitre 2. Une fois que les risques ont été évalués, le prestataire de services entamera un processus de décisions pour déterminer la nécessité de mettre en œuvre des mesures d'atténuation. Ce processus décisionnel comprend l'utilisation d'un outil de catégorisation des risques qui peut être sous la forme d'une matrice d'évaluation. Un exemple de matrice d'évaluation des risques de sécurité (index d'évaluation) est fourni dans la Figure 5-5.

5.3.56 À l'aide de cette matrice, les risques peuvent être classés selon une évaluation de leur gravité et probabilité potentielles. La méthode de la matrice d'évaluation est recommandée, mais d'autres méthodes équivalentes de description de la tolérance des risques sont disponibles. La matrice d'évaluation des risques peut être adaptée afin de tenir compte de la structure organisationnelle et des activités d'aviation de chaque prestataire de services et peut se faire sous réserve de l'accord de son autorité de réglementation. Sur la base de cet exemple de matrice, les risques considérés comme étant inacceptables (catégories rouges et jaunes) doivent être atténués afin de réduire leur gravité et/ou probabilité. Le prestataire de services devrait envisager la suspension de toutes activités qui continuent d'exposer l'organisation à des risques de sécurité intolérables en l'absence de mesures d'atténuation qui réduisent ces risques à un niveau acceptable. Des renseignements supplémentaires sur la probabilité, la gravité et sur la matrice de tolérabilité des risques sont donnés au Chapitre 2 du présent document.

5.3.57 Après l'évaluation des risques de sécurité, des mesures d'atténuation appropriées peuvent être mises en œuvre. Les mesures d'atténuation peuvent comprendre plusieurs possibilités et notamment, mais sans s'y limiter, des

modifications de procédures d'exploitation actuelles, des programmes de formation ou de l'équipement utilisé dans la fourniture de produits ou services d'aviation. D'autres solutions peuvent comprendre l'introduction de nouvelles procédures d'exploitation, de nouveaux programmes de formation, de nouvelles techniques ou contrôles de supervision. Presque invariablement, ces possibilités comprendront le déploiement ou le redéploiement des trois défenses de sécurité traditionnelles de l'aviation — la technologie, la formation et la réglementation. Une détermination de toutes conséquences involontaires, en particulier l'introduction de nouveaux dangers, devrait être faite avant la mise en œuvre de toutes mesures d'atténuation des risques.

5.3.58 Les trois stratégies génériques pour l'atténuation des risques de sécurité comprennent les éléments suivants :

- a) *Évitement*. L'activité est annulée parce que les risques de sécurité associés sont intolérables ou parce qu'ils sont jugés inacceptables par rapport aux avantages.
- b) *Réduction*. Une certaine exposition aux risques de sécurité est acceptée, quoique la gravité ou la probabilité associée aux risques soit moindre, peut-être grâce à des mesures qui atténuent les conséquences connexes.
- c) *Ségrégation de l'exposition*. Des mesures sont prises pour isoler les conséquences potentielles liées au danger ou pour établir des couches multiples de défense afin de s'en protéger.

5.3.59 Une stratégie d'atténuation des risques peut comprendre l'une des approches décrites ci-dessus ou peut inclure de multiples approches. Il est important d'envisager toute la gamme des mesures de contrôle possibles pour trouver une solution optimale. Il est nécessaire d'évaluer l'efficacité de chaque option particulière avant qu'une décision puisse être prise. Chaque option proposée d'atténuation des risques de sécurité devrait être évaluée notamment des points de vue suivants :

Probabilité du risque		Gravité du risque				
		Catastrophique A	Dangereux B	Majeur C	Mineur D	Négligeable E
Fréquent	5	5A	5B	5C	5D	5E
Occasionnel	4	4A	4B	4C	4D	4E
Éloigné	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extrêmement improbable	1	1A	1B	1C	1D	1E

Figure 5-5. Exemple d'une matrice d'évaluation (indice) de risque de sécurité

- a) *Efficacité*. Il s'agit de la mesure dans laquelle les options réduisent ou éliminent les risques de sécurité. L'efficacité peut être déterminée en termes des moyens de défense techniques, didactiques et réglementaires qui peuvent réduire ou éliminer les risques de sécurité.
- b) *Coût/bénéfice*. Il s'agit de la mesure dans laquelle les avantages perçus de l'atténuation l'emportent sur les coûts.
- c) *Caractère pratique*. Mesure dans laquelle l'atténuation peut être mise en œuvre et est pertinente en termes de technologie disponible, de ressources financières et administratives, de législations et de réglementations, de volonté politique, etc.
- d) *Acceptabilité*. Mesure dans laquelle l'option est conforme aux paradigmes des parties prenantes.
- e) *Applicabilité*. Mesure dans laquelle le respect de nouvelles règles, de nouveaux règlements ou de nouvelles procédures d'exploitation peut être suivi.
- f) *Durabilité*. Mesure dans laquelle l'atténuation sera durable et efficace.
- g) *Risques de sécurité résiduels*. Il s'agit du niveau de risque de sécurité qui demeure après la mise en place de l'atténuation initiale et qui peut nécessiter des mesures supplémentaires de maîtrise des risques.
- h) *Conséquences involontaires*. L'introduction de nouveaux dangers et des risques de sécurité connexes qui y sont associés avec la mise en œuvre de toute solution d'atténuation.

5.3.60 Une fois que l'atténuation a été approuvée et mise en œuvre, tout impact associé sur la performance de sécurité permet un retour d'information vers le processus d'assurance de la sécurité du prestataire de services. Cela est nécessaire pour garantir l'intégrité, l'efficacité et l'efficacité des défenses dans le cadre des nouvelles conditions opérationnelles.

5.3.61 Chaque exercice d'atténuation des risques doit être documenté progressivement. Cela peut être fait au moyen de diverses d'applications, qui vont de tableurs ou tableaux de base jusqu'à des logiciels commerciaux d'atténuation des risques sur mesure. Les documents d'atténuation des risques achevés devraient être approuvés par le niveau approprié de la direction. Pour un exemple de tableur de base d'atténuation des risques et des dangers, voir l'Appendice 2 au Chapitre 2.

Composant 3 du SGS. Assurance de la sécurité

5.3.62 L'assurance de la sécurité consiste en processus et activités entrepris par le prestataire de services afin de déterminer si le SGS fonctionne conformément aux attentes et aux exigences. Le prestataire de services surveille constamment ses processus internes ainsi que son environnement opérationnel afin de reconnaître les changements ou les écarts qui pourraient faire naître des risques de sécurité nouveaux ou entraîner la dégradation de contrôles existants des risques. Ces changements ou écarts peuvent alors être traités ensemble dans le cadre du processus de gestion des risques de sécurité.

5.3.63 Le processus d'assurance de la sécurité s'inscrit en complément de celui de l'assurance qualité, chacun ayant des exigences en matière d'analyse, de documentation, d'audit et d'examens de la gestion pour faire en sorte que certains critères de performance soient remplis. Alors que l'assurance qualité se concentre généralement sur le respect par l'organisation des exigences réglementaires, l'assurance qualité surveille spécifiquement l'efficacité des contrôles des risques de sécurité.

5.3.64 La relation de complémentarité de l'assurance de la sécurité et de l'assurance qualité permet l'intégration de certains processus d'appui. Cette intégration peut servir à réaliser des synergies pour garantir que les objectifs de sécurité, de qualité, et les objectifs commerciaux du prestataire de services sont réalisés.

5.3.65 Enfin, les activités d'assurance de la sécurité devraient inclure l'élaboration et la mise en œuvre d'actions correctrices pour donner suite à des constatations d'écarts systémiques qui ont un impact potentiel sur la sécurité. La responsabilité organisationnelle de l'élaboration et de la mise en œuvre de mesures correctrices devrait incomber aux départements cités dans les constatations.

Élément 3.1 du SGS Surveillance et mesure de la performance de sécurité

3.1.1 Le prestataire de services élabore et préserve les moyens de vérifier la performance de sécurité de l'organisation et de valider l'efficacité de la maîtrise des risques de sécurité.

3.1.2 La performance de sécurité du prestataire de services doit être vérifiée par référence aux indicateurs de performance de sécurité et aux cibles de performance de sécurité du SGS.

Stratégie de mise en œuvre

5.3.66 L'information utilisée pour mesurer la performance de sécurité de l'organisation est produite par ses systèmes de comptes rendus de sécurité. Les indicateurs de performance de sécurité sont examinés en détail dans la section 5.4.5 et l'Appendice 6 au présent chapitre.

5.3.67 Il existe deux types de systèmes de comptes rendus :

- a) les systèmes de comptes rendus obligatoires ;
- b) les systèmes de comptes rendus volontaires.

5.3.68 Dans les *systèmes de comptes rendus obligatoires*, il doit être rendu compte de certains types d'événements (par exemple accidents graves, incursions sur piste). Cela nécessite que soient mis en œuvre des règlements détaillés indiquant les critères de comptes rendus et les limites des événements qui doivent être déclarés. Dans les systèmes obligatoires de comptes rendus, on a tendance à recueillir plus d'informations sur des défaillances techniques à forte conséquence que sur d'autres aspects des activités opérationnelles.

5.3.69 Les *systèmes de comptes rendus volontaires* permettent de soumettre de renseignements concernant des dangers ou erreurs involontaires observés sans aucune obligation légale ou administrative de le faire. Dans ces systèmes, les agences et/ou organismes de réglementation peuvent offrir des incitations à rendre compte. Par exemple, il peut être renoncé à des mesures d'application pour des comptes rendus d'erreurs involontaires ou de violations non intentionnelles. Dans ces circonstances, l'information dont il est rendu compte ne devrait être utilisée que pour appuyer le renforcement de la sécurité. Ces systèmes sont considérés comme « non punitifs » parce qu'ils offrent une protection aux auteurs de comptes rendus, garantissant ainsi la disponibilité continue de ces renseignements pour appuyer des améliorations continues de la performance de sécurité. Alors que la nature et l'étendue des politiques non punitives des prestataires de services peut varier, l'intention consiste à promouvoir une culture efficace de compte rendu et une identification proactive des lacunes potentielles de sécurité.

5.3.70 Les systèmes de comptes rendus volontaires peuvent être confidentiels, en ce sens que toute information d'identité sur la source ne sera connue que de « dépositaires », afin de permettre des mesures de suivi. Les systèmes de comptes rendus confidentiels facilitent la mise en évidence de dangers menant à l'erreur humaine, sans crainte de « justice vengeresse » ou d'atteintes à la réputation. Les rapports volontaires d'incidents peuvent être archivés et dépersonnalisés une fois que les mesures de suivi nécessaires ont été prises. Les rapports dépersonnalisés peuvent appuyer les futures analyses de tendance afin de suivre l'efficacité de l'atténuation des risques et de repérer les dangers émergents.

5.3.71 Pour être efficaces, les outils de comptes rendus de sécurité devraient être facilement accessibles au personnel opérationnel. Le personnel opérationnel devrait recevoir une instruction portant sur les avantages des systèmes de comptes rendus de sécurité et devrait recevoir un retour d'information positif concernant les mesures correctrices prises à la suite du compte rendu. L'alignement des exigences des systèmes de comptes rendus, des outils et méthodes d'analyses peut faciliter l'échange de l'information de sécurité ainsi que des comparaisons de certains indicateurs de sécurité. Des orientations sur les systèmes de comptes rendus volontaires et confidentiels sont présentées dans l'Appendice 5 au présent chapitre.

5.3.72 D'autres sources d'information de sécurité pour appuyer la surveillance et la mesure de la performance de sécurité peuvent comprendre :

- a) Les *études sur la sécurité* sont des analyses utilisées pour acquérir une compréhension des grandes questions de sécurité ou des questions de nature mondiale. Par exemple, l'industrie des compagnies aériennes pourraient produire des recommandations de sécurité et mettre en œuvre des mesures visant à réduire les accidents et incidents pendant les phases d'approche et d'atterrissage. Les prestataires de services individuels peuvent estimer que ces recommandations globales améliorent la performance de sécurité dans le contexte de leurs activités d'aviation.
- b) Les *examens de la sécurité* sont un composant fondamental de la gestion du changement. Il est procédé à des examens de la sécurité lors de l'introduction de nouvelles technologies, de procédures nouvelles ou de changements systémiques qui touchent les opérations d'aviation. Les examens de la sécurité ont un objectif clairement défini qui est lié au changement considéré. Les examens de sécurité permettent de maintenir la performance de sécurité aux niveaux appropriés pendant les périodes de changement.
- c) Les *enquêtes sur la sécurité* examinent des éléments particuliers ou des procédures particulières d'une certaine opération. Les enquêtes sur la sécurité peuvent comprendre l'utilisation de listes de vérification, de questionnaires et d'entretiens confidentiels informels. Les enquêtes sur la sécurité fournissent généralement des informations qualitatives qui peuvent exiger une validation afin de déterminer les mesures correctrices appropriées. Néanmoins, les enquêtes peuvent constituer une source peu coûteuse de renseignements significatifs concernant la sécurité.
- d) Les *audits* se focalisent sur l'intégrité du SGS de l'organisation et de ses systèmes d'appui. Les audits offrent une évaluation de la maîtrise des risques de sécurité et des processus connexes d'assurance qualité. Les audits peuvent être menés par des entités qui sont externes au prestataire de services ou dans le cadre d'un processus d'audit interne comprenant les politiques et procédures nécessaires pour garantir son indépendance et son objectivité. Les audits sont censés donner l'assurance des fonctions de la gestion de la sécurité, et notamment le personnel, le respect des règlements approuvés, les niveaux de compétence et la formation.
- e) Les *investigations internes* portent sur certains événements de sécurité dont il doit être rendu compte, conformément aux exigences internes ou réglementaires. Les accidents et les incidents graves qui font l'objet d'investigations de la part de l'État compétent ou des autorités régionales peuvent également servir de tremplin à des enquêtes internes à entreprendre par les organisations de prestataires de services.

5.3.73 Le résultat final d'un processus de surveillance et de mesure de la performance de sécurité est l'élaboration d'indicateurs de performance de sécurité basés sur l'analyse des données recueillies grâce aux sources référencées ci-dessus. Le processus de surveillance et de mesure comprend l'utilisation d'indicateurs de performance de sécurité choisis, et de cibles de performance de sécurité et de niveaux d'alerte correspondants. Des orientations sur l'élaboration des indicateurs de performance de sécurité et leurs cibles et niveaux d'alerte sont traitées dans la Section 5.4.5 et l'Appendice 6.

Élément 3.2 du SGS La gestion du changement

Le prestataire de services élaborera et maintiendra un processus formel pour identifier les changements qui peuvent avoir une incidence sur le niveau de risque de sécurité associé à ses produits ou services d'aviation, et pour identifier et gérer les risques de sécurité qui peuvent découler de ces changements.

Stratégie de mise en œuvre

5.3.74 Les prestataires de services d'aviation connaissent des changements en raison de plusieurs facteurs, y compris, mais sans s'y limiter :

- a) l'expansion ou la contraction de l'organisation ;
- b) des modifications des systèmes, processus ou procédures internes qui appuient la fourniture des produits et services ;
- c) des changements de l'environnement opérationnel de l'organisation.

5.3.75 Le changement peut influencer sur la pertinence ou l'efficacité des stratégies existantes d'atténuation des risques de sécurité. En outre, de nouveaux dangers et les risques de sécurité y afférents peuvent être introduits involontairement dans une opération chaque fois que des changements surviennent. De tels dangers devraient être identifiés de façon à permettre l'évaluation et le contrôle de tous risques de sécurité connexes. Les examens de la sécurité, dont il a été question lors de l'analyse de la surveillance et de la mesure de la performance de sécurité, peuvent être des sources précieuses d'information pour appuyer les processus décisionnels et gérer efficacement le changement.

5.3.76 Le processus de gestion du changement de l'organisation devrait tenir compte des trois aspects suivants :

- a) *Criticité*. Les évaluations de la criticité déterminent les systèmes, l'équipement ou les activités qui sont essentiels pour la sécurité de l'exploitation des aéronefs. La criticité est normalement évaluée au cours du processus de conception du système, mais elle est aussi pertinente pendant une situation de changement. Les systèmes, l'équipement et les activités d'une plus grande criticité en matière de sécurité devraient être examinés à la suite d'un changement pour s'assurer que des mesures correctives peuvent être prises pour maîtriser les risques de sécurité qui pourraient émerger.
- b) *Stabilité des systèmes et contextes opérationnels*. Les changements peuvent être planifiés et se faire sous le contrôle direct de l'organisation. Ces changements incluent la croissance ou la contraction de l'organisation, l'expansion des produits ou services fournis, ou l'introduction de nouvelles technologies. Les changements non planifiés peuvent comprendre ceux qui sont liés aux cycles économiques, aux conflits de travail ainsi qu'aux changements du contexte politique, réglementaire ou opérationnel.

- c) *Performance passée.* La performance passée des systèmes critiques et les analyses de tendance dans le processus d'assurance de la sécurité devraient être utilisées pour anticiper et suivre la performance de sécurité en cas de changement. Le suivi de la performance passée permettra également de prendre des mesures correctrices efficaces pour s'attaquer aux lacunes en matière de sécurité repérées à la suite des audits, des évaluations, des investigations ou de rapports.

5.3.77 À mesure que les systèmes évoluent, les changements progressifs peuvent s'accumuler, exigeant alors des amendements de la description initiale du système. Par conséquent, la gestion du changement commande de revoir périodiquement la description du système et l'analyse de base des dangers afin de déterminer si elles demeurent valables.

Élément 3.3 du SGS Amélioration continue du SGS

Le prestataire de services surveillera et évaluera l'efficacité de ses processus SGS afin de permettre une amélioration continue de la performance globale du SGS.

Stratégie de mise en œuvre

5.3.78 L'amélioration continue est mesurée par la surveillance des indicateurs de performance de sécurité d'une organisation et est liée à la maturité et à l'efficacité d'un SGS. Les processus d'assurance de la sécurité appuient les améliorations du SGS grâce à une vérification et à des mesures de suivi permanentes. Ces objectifs sont réalisés par l'application d'évaluations internes et d'audits indépendants du SGS.

5.3.79 Les évaluations internes impliquent l'évaluation des activités d'aviation du prestataire de services qui peuvent fournir des renseignements utiles aux processus de décision de l'organisation. C'est à ce stade que se déroule l'activité clé du SGS — l'identification des dangers et l'atténuation des risques (HIRM). Les évaluations menées pour répondre à cette exigence doivent être effectuées par des personnes ou des organisations qui sont fonctionnellement indépendantes des processus techniques à évaluer. La fonction d'évaluation interne comprend aussi l'évaluation des fonctions de gestion de la sécurité, de définition des politiques, de gestion des risques de sécurité, d'assurance de la sécurité et de promotion de la sécurité à l'échelle de l'organisation.

5.3.80 Les audits internes comprennent l'examen systématique et régulier des activités d'aviation du prestataire de services, et notamment celles qui sont spécifiques à la mise en œuvre du SGS. Pour être les plus efficaces, les audits internes sont menés par des personnes ou des services qui sont indépendants des fonctions à évaluer. Ces audits fournissent aux responsables supérieurs, ainsi qu'aux hauts dirigeants responsables du SGS, la possibilité de suivre la mise en œuvre et l'efficacité du SGS ainsi que de ses systèmes d'appui.

5.3.81 Les audits externes du SGS peuvent être menés par des autorités pertinentes responsables de l'acceptation du SGS du prestataire de services. En outre, des audits peuvent être menés par des associations professionnelles ou d'autres tierces parties choisies par le prestataire de services. Ces audits externes renforcent le système interne d'audit et fournissent également une supervision indépendante.

5.3.82 En résumé, les processus d'évaluation et d'audit facilitent l'acquisition par le prestataire de services de l'aptitude à réaliser une amélioration continue de la performance de sécurité. La surveillance constante du SGS, de ses contrôles de sécurité et systèmes d'appui connexes permet au processus de gestion de la sécurité d'atteindre ses objectifs.

Composant 4 du SGS. Promotion de la sécurité

5.3.83 La promotion de la sécurité encourage une culture de la sécurité positive et crée un environnement propice à la réalisation des objectifs de sécurité du prestataire de services. Une culture de la sécurité positive se caractérise par des valeurs, des attitudes et un comportement qui sont résolument axés sur les efforts de sécurité de l'organisation. Pour cela, il faut une combinaison de compétences techniques qui soient constamment renforcées par la formation et l'éducation, une communication efficace et le partage de l'information. La haute direction est le chef de file de la promotion de la culture de sécurité dans l'ensemble de l'organisation.

5.3.84 Les efforts d'une organisation en faveur de la sécurité ne peuvent réussir par obligation ou par le strict respect des politiques. La promotion de la sécurité relève du comportement individuel et de celui de l'entreprise et s'inscrit en complément des politiques, procédures et processus de l'entreprise, en offrant un système de valeurs qui appuie les efforts de sécurité.

5.3.85 Le prestataire de services doit mettre en place et mettre en œuvre des processus et procédures qui facilitent une communication efficace à tous les niveaux de l'organisation. Il devrait communiquer ses objectifs de sécurité, ainsi que l'état actuel des activités et événements connexes éventuels. Le prestataire de services doit également encourager la communication « à partir du bas », en offrant un environnement qui permet à la haute direction de recevoir un retour d'information ouvert et constructif du personnel opérationnel.

Élément 4.1 du SGS Formation et éducation

4.1.1 Le prestataire de services élabore et maintient à jour un programme de formation à la sécurité pour faire en sorte que le personnel soit formé et compétent pour accomplir ses fonctions dans le cadre du SGS.

4.1.2 La portée du programme de formation à la sécurité correspondra à la participation de chaque personne au SGS.

Stratégie de mise en œuvre

5.3.86 Le directeur de la sécurité devrait fournir des informations actualisées et faciliter la formation pertinente aux questions spécifiques de sécurité auxquelles sont confrontées les unités opérationnelles. La fourniture d'une formation au personnel approprié, indépendamment de leur niveau dans l'organisation, est une indication de l'engagement de la direction vis-à-vis d'un SGS efficace. La formation à la sécurité et les programmes d'enseignement devraient comprendre les éléments suivants :

- a) les politiques, buts et objectifs de l'organisation en matière de sécurité ;
- b) les rôles et responsabilités de sécurité de l'organisation ;
- c) les principes de base de la gestion des risques de sécurité ;
- d) les systèmes de comptes rendus de sécurité ;
- e) l'appui de la gestion de la sécurité (y compris les programmes d'évaluation et d'audit) ;
- f) les lignes de communication pour la diffusion de l'information de sécurité ;

- g) un processus de validation qui mesure l'efficacité de la formation ;
- h) l'information initiale documentée et les exigences en matière de formation périodique.

5.3.87 Les programmes de formation devraient être adaptés pour répondre aux besoins et à la complexité de l'organisation et documentés pour chaque domaine d'activité. Un dossier formation devrait être établi pour chaque employé, y compris les cadres.

5.3.88 La formation à la sécurité au sein d'une organisation doit garantir que le personnel est compétent pour accomplir ses tâches de gestion de la sécurité. Les procédures de formation devraient préciser les normes de formation initiale et périodique pour le personnel opérationnel, les cadres et les superviseurs, les hauts dirigeants et le Dirigeant responsable. L'ampleur de la formation à la sécurité devrait correspondre à la responsabilité de la personne et à son implication dans le SGS. La documentation pour la formation au SGS devrait également spécifier les responsabilités en matière d'élaboration de la teneur et du calendrier de la formation et de gestion des dossiers de formation.

5.3.89 La formation devrait inclure la politique, les rôles et les responsabilités de l'organisation en matière de sécurité, les principes du SGS en matière de gestion des risques de sécurité et d'assurance de la sécurité ainsi que l'utilisation et les avantages des systèmes de comptes rendus de sécurité de l'organisation.

5.3.90 La formation à la sécurité aux hauts dirigeants devrait inclure les responsabilités en matière de sécurité, y compris le respect des exigences nationales et de celles de l'organisation en matière de sécurité, l'affectation de ressources, la réalisation d'une communication entre services en matière de sécurité et la promotion active du SGS, y compris la communication interservices relative à la sécurité. En outre, la formation à la sécurité pour les hauts dirigeants devrait comprendre des éléments sur la mise en place de cibles de performance de sécurité et de niveaux d'alerte.

5.3.91 En dernier lieu, la formation à la sécurité devrait inclure une formation particulière pour le Dirigeant responsable. Cette séance de formation devrait se faire à haut niveau, et offrir au Dirigeant responsable une compréhension du SGS et de son rapport avec la stratégie générale de l'organisation.

Élément 4.2 du SGS La communication relative à la sécurité

Le prestataire de services élaborera et préservera des moyens formels de communication en matière de sécurité permettant :

- a) d'assurer que tout le personnel a pleinement connaissance du SGS, à la mesure du poste occupé ;
- b) de transmettre l'information critique pour la sécurité ;
- c) d'expliquer pourquoi certaines mesures sont prises ;
- d) d'expliquer pourquoi des procédures de sécurité sont introduites ou modifiées.

Stratégie de mise en œuvre

5.3.92 Le prestataire de services devrait communiquer les objectifs et procédures du SGS de l'organisation à tout le personnel opérationnel. Le directeur de la sécurité devrait communiquer régulièrement par des bulletins et des

briefings des informations sur les tendances de la performance de sécurité et sur des questions spécifiques de sécurité. Il devrait aussi veiller à une large diffusion des enseignements tirés des enquêtes et des études de cas ou des expériences, tant à l'interne qu'en provenance d'autres organisations. La performance de sécurité sera plus efficace si le personnel opérationnel est activement encouragé à identifier les dangers et à en rendre compte. La communication relative à la sécurité vise donc à :

- a) faire en sorte que tout le personnel ait pleinement connaissance du SGS ;
- b) transmettre l'information critique pour la sécurité ;
- c) sensibiliser davantage les acteurs aux actions correctrices ;
- d) fournir des informations concernant des procédures de sécurité nouvelles ou modifiées.

5.3.93 Voici quelques exemples d'initiatives de communication de l'organisation :

- a) la diffusion du manuel SGS ;
- b) les processus et procédures de sécurité ;
- c) les lettres d'information, avis et bulletins sur la sécurité ;
- d) les sites web ou courriel.

5.4 PLANIFICATION DE LA MISE EN ŒUVRE DU SGS

5.4.1 Description du système

La première étape de la définition de la portée et de l'applicabilité du SGS consiste en un examen du système et en une description des éléments du SGS et de leur interface avec les systèmes et processus existants. Cette étape offre la possibilité de relever les lacunes des composants et éléments du SGS du prestataire de services. La description du système comprend les interfaces SGS au sein de l'organisation, ainsi que les interfaces pertinentes avec d'autres organisations externes, par exemple les sous-traitants. Un aperçu global de la description du système et de sa structure hiérarchique et de reddition des comptes devrait être inclus dans la documentation relative au SGS. Pour les organisations grandes et complexes, des détails des systèmes et procédures de base de l'organisation sont présentés dans les documents de présentation du prestataire de services ou dans ses manuels administratifs pertinents. Dans ces cas, il peut suffire, aux fins de la description du système, d'indiquer les grandes lignes, accompagnées d'un diagramme organisationnel avec des renvois appropriés.

5.4.2 Intégration de systèmes de gestion

5.4.2.1 Selon les contextes organisationnel, opérationnel et réglementaire, un prestataire de services peut mettre en œuvre un SGS intégré. L'intégration offre la possibilité de créer des synergies grâce à une gestion des risques de la sécurité qui couvre de multiples secteurs des activités d'aviation. Par exemple, un prestataire de services peut mettre un SGS unique pour son organisation de conception, son organisation de production, et son service de vols d'affaires. D'un autre côté, il peut y avoir des situations dans lesquelles un SGS individuel pour chaque type d'activité d'aviation est approprié. L'organisation peut définir le meilleur moyen d'intégrer ou de séparer son SGS en l'adaptant à son modèle d'affaires ou à son modèle organisationnel, sous réserve de démontrer à l'État que ses fonctions du SGS dans tous les

rôles du prestataire de services sont correctement exécutées. Le SGS du prestataire de services peut également être intégré dans des systèmes de gestion de la sécurité, de la santé et de l'environnement au travail.

Intégration du SGS et du SGQ

5.4.2.2 Le prestataire de services d'aviation déploie généralement des systèmes de gestion à l'échelle de l'entreprise. La performance de sécurité de l'organisation dépend de l'intégration efficace de ces systèmes afin d'appuyer la fourniture des produits et services. Dans le contexte du SGS, l'aspect le plus significatif de l'intégration concerne le système de gestion de la qualité (SGQ) du prestataire de services. Le SGQ est généralement défini comme étant la structure organisationnelle et les imputabilités, ressources, processus et procédures associés nécessaires pour mettre en place et promouvoir un système d'assurance continue de la qualité et d'amélioration, tout en fournissant un produit ou service. Le SGQ est actuellement exigé de la plupart des prestataires de services d'aviation, notamment en ce qui concerne l'approbation de la production (Annexe 8), les organismes de maintenance (Annexe 6, Partie I) et les prestataires de services de données météorologiques et aéronautiques (Annexes 3 et 15, respectivement).

5.4.2.3 Le SGQ et le SGS sont complémentaires. Le SGQ porte principalement sur le respect de règlements prescriptifs et d'exigences pour répondre aux attentes des clients et à des obligations contractuelles, alors que le SGS porte principalement sur la performance de sécurité. Les objectifs d'un SGS consistent à identifier les dangers liés à la sécurité, à évaluer le risque associé et à mettre en œuvre des contrôles de risques efficaces. Par contraste, le SGQ porte principalement sur la fourniture régulière de produits et services qui répondent aux spécifications pertinentes. Néanmoins, les deux systèmes SGS et SGQ :

- a) doivent être planifiés et gérés ;
- b) dépendent de la mesure et de la surveillance d'indicateurs de performance ;
- c) font intervenir toutes les fonctions de l'entreprise liées à la fourniture de produits et services d'aviation ;
- d) s'efforcent d'apporter une amélioration continue.

5.4.2.4 Le SGS et le SGQ utilisent des processus similaires de gestion des risques et d'assurance. L'objectif d'un SGS est d'identifier les dangers liés à la sécurité auxquels l'organisation doit faire face et de maîtriser les risques associés. Le SGS est conçu pour gérer le risque de sécurité et mesurer la performance de sécurité pendant la fourniture des produits et services. Le processus de gestion des risques de sécurité élimine les dangers ou met en place des contrôles efficaces pour atténuer les risques de sécurité en maintenant un équilibre approprié de l'allocation des ressources entre la production et la protection pour répondre aux exigences en matière de performance de sécurité.

5.4.2.5 Le SGQ assure la régularité de la fourniture des produits et services afin de respecter les normes de performance ainsi que les attentes des clients. Le SGQ dispose également d'une fonction d'assurance indépendante qui utilise un processus de rétro-information pour assurer la fourniture des produits et services qui sont « adaptés aux objectifs » et exempts de défauts ou d'erreurs. La fonction d'assurance de la qualité repère les processus et procédures inefficaces dont la conception doit être revue pour plus d'efficacité et d'efficience.

5.4.2.6 En outre, le SGS et le SGQ utilisent des outils analogues. Les praticiens de la sécurité et de la qualité se concentrent essentiellement sur le même objectif de fournir des produits et services sûrs et fiables aux clients. Les praticiens de la qualité et de la sécurité sont formés à diverses méthodes d'analyses, y compris l'analyse des causes profondes et l'analyse statistique des tendances.

5.4.2.7 Compte tenu des aspects complémentaires du SGS et du SGQ, il est possible d'établir un lien synergique entre les deux systèmes, qui peut être résumé comme suit :

- a) un SGS est appuyé par des processus de SGQ comme l'audit, l'inspection, l'enquête, l'analyse des causes profondes, la conception des processus, l'analyse statistique et les mesures préventives ;
- b) un SGQ peut prévoir des questions de sécurité qui existent en dépit du respect par l'organisation des normes et des spécifications ;
- c) les principes, politiques et pratiques de qualité sont liés aux objectifs de la gestion de la sécurité.

5.4.2.8 Du fait de la relation entre le SGS et le SGQ, chaque système fait des contributions complémentaires à la réalisation des objectifs de sécurité et de qualité de l'organisation. Une comparaison sommaire des deux systèmes est présentée dans le Tableau 5-1.

Tableau 5-1. Comparaison sommaire du SGQ et du SGS

SGQ	SGS
Qualité	Sécurité
Assurance de qualité	Assurance de sécurité
Contrôle de la qualité	Identification des dangers et contrôle des risques
Culture de la qualité	Culture de la sécurité
Respect des exigences	Niveau acceptable de performance de sécurité
Prescriptif	Basé sur les performances
Normes et spécifications	Facteurs organisationnels et humains
Réactif > Proactif	Proactif > Prédicatif

5.4.3 Analyse des écarts

5.4.3.1 L'analyse des écarts compare les procédés et procédures actuelles de gestion de la sécurité du prestataire de services aux exigences qui figurent dans le cadre du SGS. Le prestataire de services d'aviation a généralement mis en œuvre diverses fonctions SGS par respect des règlements nationaux ou à la suite de l'adoption des meilleures pratiques de l'industrie. L'élaboration d'un SGS devrait se fonder sur les structures et systèmes de contrôle existants de l'organisation. L'analyse des écarts facilite l'élaboration d'un plan de mise en œuvre du SGS en repérant les écarts qui doivent être corrigés pour mettre en œuvre pleinement un SGS. Une fois que l'analyse des écarts a été achevée et pleinement documentée, les ressources et les processus qui ont été repérés comme manquants ou insuffisants constitueront la base du plan de mise en œuvre du SGS.

5.4.3.2 L'Appendice 7 au présent chapitre donne une liste des questions de l'analyse des écarts afin d'aider le prestataire de services à évaluer systématiquement ses processus existants. À partir d'une réponse objective à chaque question de l'analyse des écarts, les renforcements ou les mesures qui s'imposent apparaîtront clairement.

5.4.4 Plan de mise en œuvre du SGS

5.4.4.1 Un plan de mise en œuvre du SGS est élaboré en consultation avec le Dirigeant responsable et les gestionnaires responsables de la fourniture des produits et services liés ou apportant leur concours à la sécurité de l'exploitation des aéronefs. Une fois le plan achevé, le Dirigeant responsable l'entérine. Le plan de mise en œuvre du SGS comprend des délais et des jalons conformes aux exigences identifiées dans le processus d'analyse des écarts, à la taille du prestataire de services et à la complexité de ses produits ou services. Le plan devrait traiter de la coordination avec les organismes ou sous-traitants externes, le cas échéant.

5.4.4.2 Le plan de mise en œuvre du prestataire de services peut être documenté sous diverses formes, depuis une simple fiche de calcul jusqu'à un logiciel spécialisé de gestion de projet. Le plan de mise en œuvre devrait traiter des écarts jusqu'à l'achèvement des mesures spécifiques et des jalons conformément aux délais indiqués. L'affectation de chaque tâche garantira l'imputabilité d'un bout à l'autre du processus de mise en œuvre. Le plan devrait être revu régulièrement et actualisé au besoin. Un exemple de présentation d'un plan/calendrier de mise en œuvre du SGS est présenté dans l'Appendice 7 au présent chapitre.

5.4.4.3 La mise en œuvre complète de tous les composants et éléments du cadre du SGS peut prendre jusqu'à cinq ans, selon le degré de maturité et la complexité d'une organisation. La mise en œuvre du SGS, et notamment les orientations relatives à une approche progressive, sont examinées dans la Section 5.5.

5.4.5 Indicateurs de performances de sécurité

5.4.5.1 Un SGS définit des résultats de performance mesurables afin de déterminer si le système fonctionne vraiment conformément aux attentes de conception et au lieu de répondre simplement aux exigences réglementaires. Les indicateurs de performance de sécurité sont utilisés pour surveiller les risques de sécurité connus, détecter les risques de sécurité émergents et déterminer les mesures correctrices éventuelles à prendre.

5.4.5.2 Les indicateurs de performance de sécurité offrent également des preuves objectives pour que le régulateur puisse évaluer l'efficacité du SGS du prestataire de services et suivre la réalisation de ses objectifs de sécurité. Les indicateurs de performance de sécurité du prestataire de services considèrent des facteurs comme la tolérance de risques de sécurité de l'organisation, les coûts/avantages de la mise en œuvre d'améliorations du système, les exigences réglementaires et les attentes du public. Les indicateurs de performance de sécurité devraient être choisis et élaborés en consultation avec l'autorité de réglementation du prestataire de services. Ce processus est nécessaire afin de faciliter le regroupement et l'harmonisation par le régulateur des indicateurs de performance de sécurité du prestataire de services pour le même secteur d'aviation.

5.4.5.3 Les indicateurs de performance de sécurité et cibles associés devraient être acceptés par l'État responsable de l'autorisation, de la certification ou de la désignation du prestataire de services. Les indicateurs de performance de sécurité sont complémentaires à toute exigence légale ou réglementaire et ne dégagent pas le prestataire de services de ses obligations réglementaires.

5.4.5.4 Dans la pratique, la performance de sécurité d'un SGS est exprimée par les indicateurs de performance de sécurité et leurs valeurs d'alerte et de cibles correspondantes. Le prestataire de services devrait surveiller la performance des indicateurs actuels dans le contexte des tendances historiques, afin de repérer tous changements anormaux de la performance de sécurité. De même, les réglages de cibles et d'alerte devraient tenir compte de la performance historique récente pour un indicateur donné. Les objectifs d'améliorations souhaités devraient être réalistes et réalisables pour le prestataire de services et le secteur d'aviation associé.

5.4.5.5 L'établissement d'un niveau d'alerte pour un indicateur de sécurité est utile pour la surveillance des risques. Un niveau d'alerte est un critère commun pour distinguer les zones de performance acceptables des zones inacceptables d'un indicateur de sécurité donné. Selon la littérature sur la mesure de la sécurité, une méthode objective

fondamentale pour établir les critères d'alerte hors contrôle (OOC) est l'utilisation du principe de l'écart type. Cette méthode tient compte de l'écart type et des valeurs moyennes des points de données historiques précédents pour un indicateur de sécurité donné. Ces deux valeurs sont alors utilisées pour établir le niveau d'alerte pour la prochaine période de surveillance de l'indicateur.

5.4.5.6 Une gamme d'indicateurs de performance de sécurité à fortes conséquences et à faibles conséquences offre une connaissance plus complète de la performance de sécurité du prestataire de services. Cela garantira que les résultats à fortes conséquences (par exemple des accidents et des incidents graves) ainsi que des événements à faibles conséquences (par exemple des incidents, des rapports de non-conformité, des écarts) sont traités. Les indicateurs de performance de sécurité sont essentiellement des diagrammes de données de tendances qui suivent les occurrences en termes de taux d'événements (par exemple nombre d'incidents par 1 000 FH). Les indicateurs à fortes conséquences devraient être traités en premier, alors que les indicateurs à faibles conséquences peuvent être élaborés lors de la phase plus avancée de la mise en œuvre du SGS.

5.4.5.7 Une fois que les indicateurs de performance de sécurité et leurs niveaux cibles et niveaux d'alerte correspondants ont été définis, le résultat de performance de chaque indicateur devrait être actualisé et surveillé régulièrement. Le niveau cible et le niveau d'alerte de chaque indicateur peuvent être suivis en termes de leur état respectif de performance. Un récapitulatif de la performance globale des cibles et des alertes de l'ensemble des indicateurs de performance de sécurité peut également être compilé/agrégé pour une période de surveillance donnée. Des valeurs qualitatives (satisfaisant/insatisfaisant) peuvent être attribuées pour chaque « cible atteinte » et chaque « niveau d'alerte non franchi ». Autrement, des valeurs numériques (points) peuvent être utilisées pour donner une mesure quantitative de la performance globale de l'ensemble des indicateurs. Des exemples d'indicateurs de performance de sécurité et leurs critères de niveaux cibles et niveau d'alerte sont fournis dans l'Appendice 6 au présent chapitre.

5.5 MÉTHODE DE MISE EN ŒUVRE PAR PHASES

5.5.1 Généralités

5.5.1.1 L'objectif de la présente section est de présenter un exemple des quatre phases de mise en œuvre du SGS. La mise en œuvre d'un SGS est un processus systématique. Néanmoins, ce processus peut être une tâche ardue selon les facteurs, comme la disponibilité d'éléments indicatifs et de ressources requis pour la mise en œuvre, ainsi que de la connaissance préalable par le prestataire de services des processus et procédures du SGS.

5.5.1.2 Les raisons d'une approche progressive de la mise en œuvre du SGS comprennent :

- a) l'établissement d'une série gérable d'étapes à suivre pour mettre en œuvre un SGS, y compris l'attribution des ressources ;
- b) la nécessité de permettre la mise en œuvre d'éléments du cadre SGS dans des séquences diverses, selon les résultats de l'analyse des écarts de chaque prestataire de services ;
- c) la disponibilité initiale de données et de processus analytiques pour appuyer des pratiques réactives, proactives et prédictives de gestion de la sécurité ;
- d) la nécessité d'un processus méthodique pour garantir une mise en œuvre efficace et durable du SGS.

5.5.1.3 L'approche par phases reconnaît que la mise en œuvre d'un SGS bien au point est un processus qui s'étend sur plusieurs années. Une approche de mise en œuvre par phase permet au SGS de devenir plus solide à mesure que chaque phase de mise en œuvre est achevée. Les processus fondamentaux de gestion de la sécurité sont achevés avant de passer aux phases successives qui font intervenir des processus d'une complexité supérieure.

5.5.1.4 Quatre phases de mise en œuvre sont proposées pour un SGS. Chaque phase est associée à divers composants (ou éléments) conformément au cadre SGS de l'OACI. Il est clair que la configuration spécifique d'éléments dans les présents éléments indicatifs n'entend pas être absolue. Les États et les prestataires de services peuvent choisir d'apporter des modifications aux circonstances, comme il conviendra. Un résumé des quatre phases de mise en œuvre du SGS et de leurs éléments correspondants figure dans le Tableau 5-2.

5.5.2 Phase 1

5.5.2.1 L'objectif de la Phase I de mise en œuvre du SGS est d'établir un plan général de la façon de remplir les exigences du SGS et de les intégrer dans les systèmes de contrôle de l'organisation, ainsi qu'un cadre d'imputabilité pour la mise en œuvre du SGS.

5.5.2.2 Pendant la Phase I, la planification de base et l'attribution des responsabilités sont établies. L'analyse des écarts est au centre de la Phase I. À partir de cette analyse, une organisation peut déterminer l'état en cours de ses processus de gestion de la sécurité et entreprendre une planification détaillée pour le développement d'autres processus de gestion de la sécurité. Un extrait important de la Phase I est le plan de mise en œuvre du SGS.

5.5.2.3 À l'achèvement de la Phase I, les activités suivantes devraient être finalisées d'une façon qui réponde aux attentes de l'autorité de supervision de l'aviation civile, comme indiqué dans les spécifications et éléments d'orientation pertinents :

Engagement et responsabilité de la direction — Élément 1.1 i)

- a) Identifier le Dirigeant responsable et les imputabilités des gestionnaires de la sécurité en matière de sécurité. Cette activité est basée sur les Éléments 1.1 et 1.2 du cadre SGS de l'OACI.
- b) Mettre en place une équipe de mise en œuvre du SGS. Cette équipe devrait comprendre des représentants des services pertinents. Le rôle de l'équipe consiste à impulser la mise en œuvre du SGS de l'étape de la planification jusqu'à sa mise en œuvre finale. D'autres fonctions de l'équipe de mise en œuvre comprendront, mais sans s'y limiter :
 - 1) l'élaboration du plan de mise en œuvre du SGS ;
 - 2) s'assurer que l'équipe reçoit la formation SGS adéquate et dispose des compétences techniques suffisantes pour mettre en œuvre efficacement les éléments du SGS et processus connexes ;
 - 3) assurer le suivi et rendre compte des progrès de la mise en œuvre du SGS, fournir des mises à jour régulières et coordonner les activités avec le Dirigeant responsable du SGS.
- c) Définir la portée des activités de l'organisation (services/divisions) auxquelles le SGS sera applicable. La portée de l'applicabilité du SGS de l'organisation devra ultérieurement être décrite dans le document SGS, comme il convient. Cette activité est basée sur l'Élément 1.5 du cadre SGS de l'OACI. Des orientations sur la description du système sont fournies au § 5.4.1 du présent chapitre.
- d) Procéder à une analyse des écarts des systèmes et processus actuels de l'organisation par rapport aux exigences du cadre SGS de l'OACI (ou des dispositions réglementaires pertinentes concernant le SGS). Des orientations sur une analyse des écarts du SGS pour un prestataire de services sont présentées dans l'Appendice 7 au présent chapitre.

Plan de mise en œuvre du SGS — Élément 1.5 i)

- a) Élaborer un plan de mise en œuvre du SGS expliquant comment l'organisation mettra en œuvre le SGS sur la base des lacunes du système et des procédés qui ont été constatés et qui résultent de l'analyse des écarts. Un exemple d'un plan de mise en œuvre de base du SGS est fourni dans l'Appendice 7 au présent chapitre.

Nomination du personnel clé de sécurité — Élément 1.3

- a) Désigner la personne clé pour le SGS (fonction sécurité/qualité) dans l'organisation qui sera chargée de l'administration du SGS au nom du Dirigeant responsable.
- b) Établir le bureau des services de sécurité.

Formation et éducation — Élément 4.1 i)

- a) Procéder à une analyse des besoins de formation.
- b) Organiser et mettre en place des calendriers de formation appropriée pour tout le personnel, en fonction de leurs responsabilités individuelles et de leur implication dans le SGS.
- c) Élaborer la formation à la sécurité en tenant compte :
 - 1) de la formation initiale particulière à un emploi (sécurité générale) ;
 - 2) de la formation périodique.
- d) Préciser les coûts associés à la formation.
- e) Élaborer un processus de validation qui mesure l'efficacité de la formation.
- f) Mettre en place un système de dossiers de la formation à la sécurité.

La communication en matière de sécurité — Élément 4.2 i)

- a) Instaurer un mécanisme ou un moyen pour la communication en matière de sécurité.
- b) Mettre en place un moyen de diffuser l'information de sécurité :
 - 1) par des lettres d'information, avis et bulletins ;
 - 2) au moyen de sites Web ;
 - 3) par courrier électronique.

5.5.3 Phase 2

L'objectif de la Phase 2 est de mettre en œuvre des processus essentiels de gestion de la sécurité, tout en corrigeant des défaillances potentielles des processus existants de gestion de la sécurité. La plupart des organisations ont généralement des activités de base de gestion de la sécurité en place à divers niveaux de mise en œuvre. Cette phase a pour but de regrouper les activités existantes et de développer celles qui n'existent pas encore.

Engagement et responsabilité de la direction — Élément 1.1 ii)

- a) Élaborer une politique de sécurité.
- b) Faire signer la politique de sécurité par le Dirigeant responsable.
- c) Communiquer la politique de sécurité dans toute l'organisation.
- d) Mettre en place un calendrier d'examens de la politique de sécurité pour garantir qu'elle reste pertinente et appropriée à l'organisation.
- e) Établir des objectifs de sécurité pour le SGS en élaborant des normes de performance de sécurité, en termes :
 - 1) d'indicateurs de performance de sécurité ;
 - 2) de cibles et de niveau d'alerte de performance de sécurité ;
 - 3) de plans d'action.
- f) Établir les besoins du SGS en matière de sous-traitants :
 - 1) établir une procédure pour inscrire les besoins du SGS dans le processus de sous-traitance ;
 - 2) établir les besoins du SGS dans le dossier d'appels d'offres.

Imputabilités en matière de sécurité — Élément 1.2

- a) Définir les imputabilités en matière de sécurité et les communiquer dans toute l'organisation.
- b) Mettre en place le groupe d'action pour la sécurité (SAG).
- c) Mettre en place le comité de coordination du SGS/sécurité.
- d) Définir des fonctions claires pour le SAG et le comité de coordination du SGS/sécurité.
- e) Établir les lignes de communication entre le bureau des services de sécurité, le Dirigeant responsable, le SAG et le comité de coordination du SGS/sécurité.
- f) Nommer le Dirigeant responsable comme président du comité de coordination du SGS/sécurité.
- g) Élaborer un calendrier de réunions entre le bureau des services de sécurité et le comité de coordination du SGS/sécurité et le SAG, selon les besoins.

Coordination de la planification des interventions d'urgence — Élément 1.4

- a) Examiner l'ébauche de l'ERP s'agissant de la délégation de pouvoirs et de l'affectation des responsabilités en cas d'urgence.
- b) Établir les procédures de coordination des mesures par le personnel clé lors d'une situation d'urgence et le retour aux opérations normales.
- c) Indiquer les entités externes qui interagiront avec l'organisation pendant les situations d'urgence.
- d) Évaluer les ERP respectifs des entités externes.
- e) Établir la coordination entre les différents ERP.
- f) Incorporer les renseignements sur la coordination entre les différents ERP dans la documentation relative au SGS de l'organisation.

Note.— Voir l'Appendice 3 pour d'autres orientations sur l'ERP.

Documentation relative au SGS — Élément 1.5 ii)

- a) Créer un système de documentation du SGS afin de décrire, de stocker, d'extraire et d'archiver toutes les informations et tous les dossiers liés au SGS :
 - 1) en élaborant un document SGS qui sera soit un manuel autonome ou une section distincte dans un manuel existant sous l'autorité de l'organisation (voir l'Appendice 4 pour des orientations sur l'élaboration de manuel SGS) ;
 - 2) mettre en place un système de classement du SGS afin de recueillir et de tenir à jour des dossiers actualisés sur les processus SGS permanents de l'organisation ;
 - 3) tenir des dossiers afin de constituer une référence historique et de présenter l'état actuel de tous les processus SGS comme : un registre des dangers, un index des évaluations de la sécurité achevées ; des dossiers sur la formation à la sécurité/SGS ; des SPI actuels et les objectifs de sécurité associés ; des rapports d'audit interne sur le SGS ; les procès-verbaux des réunions du comité de la sécurité/SGS et le plan de mise en œuvre du SGS ;
 - 4) tenir des dossiers qui serviront de preuve du fonctionnement et des activités du SGS pendant l'évaluation ou audit interne ou externe du SGS.

5.5.4 Phase 3

L'objectif de la Phase 3 est de mettre en place les processus de gestion des risques de sécurité. Vers la fin de la Phase 3, l'organisation sera prête à recueillir des données sur la sécurité et à procéder à des analyses de sécurité sur la base des renseignements obtenus grâce aux divers systèmes de comptes rendus.

Identification des dangers — Élément 2.1 i)

- a) Mettre en place une procédure de comptes rendus volontaires. Voir l'Appendice 5 pour les orientations.
- b) Mettre en place un programme/calendrier d'examens systématiques de tous les processus/équipements applicables liés à la sécurité de l'aviation auxquels le processus HIRM peut être appliqué.
- c) Établir un procédé de priorisation et d'affectation des dangers identifiés, aux fins de l'atténuation des risques.

Évaluation et atténuation des risques de sécurité — Élément 2.2

- a) Mettre en place une procédure de gestion des risques de sécurité, y compris son processus d'approbation et d'examen périodique.
- b) Élaborer et adopter des matrices de risques de sécurité pertinentes aux processus opérationnels ou de production de l'organisation.
- c) Inclure les matrices de risques de sécurité et instructions associées dans le SGS de l'organisation ou dans les éléments didactiques sur la gestion des risques.

Surveillance et mesure de la performance de sécurité — Élément 3.1 i)

- a) Mettre en place une procédure interne de comptes rendus d'enquêtes sur les événements. Cette procédure peut inclure des comptes rendus obligatoires ou des comptes rendus de défaillance majeure, selon le cas.
- b) Mettre en place la collecte, le traitement et l'analyse des données sur la sécurité dans le cas des résultats à fortes conséquences.
- c) Mettre en place des indicateurs de sécurité à hautes conséquences (ALoSP initial) et leurs niveaux cibles et niveaux d'alerte associés. Des exemples d'indicateurs de la sécurité à hautes conséquences sont les taux d'accidents, les taux d'incidents graves et la surveillance des résultats de non-conformité à risques élevés. Voir l'Appendice 6 pour des orientations sur les indicateurs de performance de sécurité.
- d) Parvenir à un accord avec l'autorité de supervision de l'État en ce qui concerne les indicateurs de performance de sécurité et les cibles de performance de sécurité.

La gestion du changement — Élément 3.2

- a) Mettre en place un processus formel de gestion du changement qui tienne compte :
 - 1) de la vulnérabilité des systèmes et activités ;
 - 2) de la stabilité des systèmes et des environnements opérationnels ;

- 3) de la performance passée ;
 - 4) des changements réglementaires, industriels et technologiques.
- b) Veiller à ce que les procédures de gestion du changement traitent de l'impact sur les dossiers existants de performance de sécurité et d'atténuation des risques avant la mise en œuvre de nouveaux changements.
 - c) Mettre en place des procédures pour s'assurer que l'évaluation de la sécurité des nouvelles opérations, de nouveaux processus et des nouveaux équipements liés à la sécurité de l'aviation soit menée (ou prise en compte) selon le cas, avant d'être mises en service.

Amélioration continue du SGS — Élément 3.3 i)

- a) Élaborer des formulaires d'évaluations internes.
- b) Définir un processus d'audit interne.
- c) Définir un processus d'audit externe.
- d) Définir un calendrier de l'évaluation des installations, de l'équipement, de la documentation et des procédures, à mettre en place grâce à des audits et des enquêtes.
- e) Élaborer la documentation pertinente à l'assurance de la sécurité de l'exploitation.

5.5.5 Phase 4

La Phase 4 est la phase finale de la mise en œuvre du SGS. Cette phase comprend la mise en œuvre réussie de la gestion des risques de sécurité et de l'assurance de la sécurité. Dans cette phase, l'assurance de la sécurité opérationnelle est évaluée par la mise en œuvre de surveillance régulière, de retour d'information et de mesures correctrices continues afin de maintenir l'efficacité des contrôles des risques de sécurité.

Engagement et responsabilité de la direction — Élément 1.1 iii)

- a) Renforcer la procédure/politique disciplinaire existante en tenant dûment compte des erreurs/fautes involontaires à distinguer des violations délibérées/flagrantes.

Identification des dangers — Élément 2.1 ii)

- a) Intégrer les dangers identifiés à partir des rapports d'enquêtes sur les événements dans le système de comptes rendus volontaires.
- b) Intégrer l'identification des dangers et les procédures de gestion de risques dans le SGS du sous-traitant ou du client, selon le cas.

- c) Au besoin, élaborer un processus d'établissement de priorités des dangers recensés, en vue de l'atténuation des risques sur la base des domaines dans lesquels les besoins ou les préoccupations sont les plus grands. Voir l'Appendice 3 au Chapitre 2 pour les orientations.

Surveillance et mesure de la performance de sécurité — Élément 3.1 ii)

- a) Renforcer le système de collecte et de traitement des données sur la sécurité afin d'inclure les événements à faibles conséquences.
- b) Établir des indicateurs de sécurité/qualité à faibles conséquences, avec une surveillance des niveaux cibles et niveaux d'alerte, selon le cas (ALoSP bien défini).
- c) Conclure un accord avec l'autorité de supervision de l'État sur les indicateurs de performance de sécurité à faibles conséquences et les niveaux cibles et niveaux d'alerte de performance de sécurité.

Amélioration continue du SGS — Élément 3.3 ii)

- a) Établir des audits du SGS ou les intégrer dans les programmes actuels d'audits internes et externes existants.
- b) Établir d'autres programmes d'examins/enquêtes sur le SGS opérationnel, selon le cas.

Formation et éducation — Élément 4.1 ii)

- a) Achever un programme de formation au SGS pour tout le personnel pertinent.

La communication en matière de sécurité — Élément 4.2 ii)

- a) Établir des mécanismes pour promouvoir le partage et l'échange de renseignements sur la sécurité à l'interne et à l'externe.

5.5.6 Éléments du SGS mis en œuvre progressivement au cours des Phases 1 à 4

Dans la mise en œuvre par phase, les trois éléments clés ci-après sont mis en œuvre progressivement dans le cadre de chaque phase :

Documentation relative au SGS — Élément 1.5

À mesure que le SGS mûrit progressivement, le manuel SGS pertinent et la documentation relative à la sécurité doivent être révisés et mis à jour en conséquence. Cette activité sera inhérente à toutes les phases de la mise en œuvre du SGS et doit être maintenue après la mise en œuvre également.

Formation et éducation — Élément 4.1 et communication relative à la sécurité — Élément 4.2

Comme pour la documentation relative au SGS, la formation, l'éducation et la communication relatives à la sécurité sont des activités permanentes importantes dans toutes les phases de la mise en œuvre du SGS. À mesure que le SGS évolue, de nouveaux procédés, procédures ou règlements peuvent entrer en vigueur ou des procédures existantes peuvent changer pour tenir compte des besoins du SGS. Pour s'assurer que ces changements sont effectivement compris et mis en œuvre par tout le personnel impliqué dans des fonctions liées à la sécurité, il est indispensable que la formation et la communication restent des activités permanentes pendant toute la durée de la mise en œuvre complète du SGS et par la suite.

Appendice 1 au Chapitre 5

SIGNATURES ÉLECTRONIQUES

Note.— Le présent appendice contient des extraits de la Circulaire consultative AC N° 120-78 de l'Administration fédérale de l'aviation des États-Unis (FAA) « Acceptance and Use of Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manuals » (Acceptation et utilisation de signatures électroniques, de systèmes électroniques de gestion des dossiers et de manuels électroniques), en date du 29 octobre 2002¹. Il est entendu que les informations communiquées ci-dessous le sont uniquement à titre d'illustration et n'ont aucun caractère restrictif. Cet appendice n'est pas censé être pris ou utilisé comme unique ensemble de renseignements nécessaires pour l'utilisation de signatures électroniques. Le présent appendice ne porte pas atteinte au droit des États contractants d'élaborer et/ou d'utiliser leurs propres éléments sur les signatures électroniques.

1. Quel est l'objet de cette circulaire consultative (AC) ?

- a) Cette AC n'est pas obligatoire et ne constitue pas un règlement. Elle contient des éléments indicatifs sur l'acceptation et l'utilisation de signatures électroniques en vue de répondre à certains besoins opérationnels et de maintenance. L'AC fournit également des indications sur l'acceptabilité des systèmes électroniques de gestion des dossiers et de manuels de maintenance électroniques, y compris les manuels des procédures d'inspection, d'assurance de la qualité, les manuels d'exploitation et les manuels de formation exigés en vertu du Titre 14 du Code des règlements fédéraux (CFR 14)...
- b) L'AC décrit un moyen acceptable, mais non unique, de respecter les exigences opérationnelles et de maintenance de la FAA. Plus précisément, les signatures manuelles, les dossiers manuels et cachets mécaniques continuent d'être acceptables. Toutefois, si vous utilisez le moyen électronique décrit dans l'AC, vous devez vous y confirmer à tous les égards importants.

2. À qui s'applique cette AC ?

- Transporteurs aériens au titre du CFR 14, Parties 121, 129 ou 135.
- Aux exploitants au titre du CFR 14, Parties 91, 125, 133 ou 137.
- Aux personnes qui accomplissent la certification des hommes de l'air au titre du CFR 14, Parties 61, 63, 65, 141 et 142.
- Aux personnes qui effectuent la maintenance ou la maintenance préventive au titre du CFR 14, Partie 43.
- Aux ateliers de réparation au titre du CFR 14, Partie 145.

1. Le texte complet de la circulaire FAA AC N° 120-78 peut être trouvé sur le site de la FAA : http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/23224.

- Aux écoles techniques de maintenance d'aviation au titre du CFR 14, Partie 147.

3. Définitions

...

- d) **Signature numérique.** Données générées cryptographiquement, qui identifient le signataire d'un document (signataire) et certifient que le document n'a pas été altéré. La technologie des signatures numériques constitue le fondement d'une diversité de produits de sûreté, d'entreprises électroniques et de commerces électroniques. Cette technologie est fondée sur le chiffrement à clé publique/privée, technologie de signature numérique utilisée dans la messagerie sécurisée, l'infrastructure à clé publique (PKI), les réseaux privés virtuels (VPN), qui sont les normes de l'internet pour les transactions sécurisées et les signatures numériques électroniques.
- e) **Signature électronique.** Il s'agit de l'équivalent en ligne d'une signature manuelle. Il s'agit d'un son, d'un symbole ou d'un processus électronique attaché ou logiquement associé à un contrat ou autre dossier et exécuté ou adopté par une personne. Elle identifie et authentifie électroniquement une personne qui saisit, vérifie ou audite des dossiers informatisés. Une signature électronique combine des fonctions de chiffrement de signature numérique avec l'image de la signature manuelle d'une personne ou une autre marque visible considérée comme acceptable dans un processus traditionnel de signature. Elle authentifie les données avec un algorithme de hachage et constitue une authentification permanente et sûre de l'utilisateur.

...

5. Qu'est-ce qu'une signature électronique acceptable ?

- a) **Généralité.** Avant de récents changements permettant l'utilisation de signatures électroniques, les signatures manuelles étaient utilisées sur n'importe quel dossier, saisie ou document. L'objet de la signature électronique est identique à celui d'une signature manuelle ou de toute autre forme de signature actuellement acceptée par la FAA. La signature manuelle est universellement acceptée car elle a certaines qualités et attributs (par exemple alinéa c 4) d) ci-dessous concernant la cessation d'emploi) qui devraient être préservés dans n'importe quelle signature électronique. Par conséquent, une signature électronique devrait posséder ces qualités et attributs qui garantissent l'authenticité d'une signature manuelle.

- b) **Formes de signatures électroniques.**

1) Une signature électronique peut se présenter sous les formes suivantes :

- une signature numérique ;
- une image numérisée d'une signature papier ;
- une notation dactylographiée ;
- un code électronique ;
- toute autre forme unique d'identification individuelle qui peut être utilisée comme moyen d'authentifier un dossier, une saisie ou un document.

- 2) Les données d'identification personnelles que l'on trouve dans un système électronique ne peuvent pas toutes être considérées comme une signature. Par exemple, la saisie du nom d'une personne dans un système électronique peut ne pas constituer une signature électronique. D'autres garanties égales à celles d'une signature manuelle devraient être fournies.
- c) **Attributs d'une signature électronique acceptable.** D'abord, une signature électronique doit faire partie d'un programme bien conçu. Ce programme devrait, au minimum, tenir compte des éléments suivants.
- 1) **Unicité.** Une signature électronique devrait garder les qualités d'une signature manuelle qui garantissent son unicité. Une signature devrait identifier une personne précise et être difficile à contrefaire. Une signature unique est une preuve qu'une personne approuve une déclaration. Un système électronique ne peut fournir une identification unique avec une certitude raisonnable, à moins que l'identification soit difficile à reproduire par une personne non autorisée...
 - 2) **Importance.** Une personne qui utilise une signature électronique devrait prendre activement des mesures reconnaissables pour apposer sa signature. Des mesures acceptables, délibérées de création d'une signature électronique numérique comprennent, mais sans s'y limiter :
 - l'utilisation d'une carte magnétique ;
 - la signature d'un document électronique avec un crayon électronique ;
 - la frappe de touches spécifiques du clavier ;
 - l'utilisation d'une signature numérique.
 - 3) **Portée.** La portée de l'information qui est approuvée par une signature électronique devrait être claire pour le signataire et pour les lecteurs ultérieurs du dossier, de la saisie ou du document. Dans les documents écrits, la signature est proche des renseignements, afin d'identifier les éléments qui sont attestés par la signature. Toutefois, les documents électroniques peuvent ne pas placer la signature de la même façon. Il est donc important de clairement identifier les sections spécifiques d'un dossier ou document qui sont approuvées par une signature, par rapport aux sections qui ne le sont pas. Les méthodes acceptables d'indiquer les zones concernées comprennent, mais sans s'y limiter, le surlignement, l'inversion du contraste ou l'utilisation de bordures ou de caractères clignotants. En outre, le système devrait notifier au signataire que la signature a été apposée...
 - 4) **Sûreté de la signature.** La sûreté de la signature manuelle d'une personne est maintenue en vérifiant qu'il est difficile à un autre individu de la contrefaire ou de l'altérer. Une signature électronique devrait maintenir un niveau équivalent de sûreté. Un système électronique qui produit des signatures devrait empêcher d'autres personnes d'apposer la signature d'une autre personne sur un dossier, une saisie ou un document...
 - 5) **Non-répudiation.** Une signature électronique devrait empêcher un signataire de nier qu'il a apposé une signature sur un dossier, une saisie ou un document spécifique. Plus il est difficile de contrefaire une signature, plus il est vraisemblable que la signature a été créée par le signataire. Les dispositifs de sûreté du système qui rendent difficiles à d'autres la copie de signatures ou l'altération de documents signés garantissent généralement qu'une signature a effectivement été faite par le signataire...

- 6) **Traçabilité.** Une signature électronique devrait assurer une traçabilité positive jusqu'à la personne qui a signé un dossier, une saisie ou un autre document quelconque.
- d) **Autres formes acceptables de signature/identification.** Même si la présente circulaire porte expressément sur les signatures électroniques, d'autres types de signatures, par exemple un cachet mécanique, peuvent également être acceptables à la FAA. Si une identification autre qu'une signature manuelle est utilisée, l'accès à cette identification devrait être limité uniquement à la personne nommée.
- e) **Respect des autres exigences réglementaires.** Bien que la FAA permette maintenant l'utilisation de signatures électroniques pour répondre à certains besoins opérationnels et de maintenance de la FAA, n'importe quel matériel informatique utilisé pour générer les documents et dossiers requis doit continuer à respecter les exigences réglementaires en vigueur. Une signature correcte apposée à un document créé de manière incorrecte aboutit de toute façon à un document qui n'est pas conforme aux exigences réglementaires. Les méthodes et procédures utilisées pour générer une signature électronique doivent donc satisfaire à toutes les exigences réglementaires d'un système de dossiers qui sera utilisé par des propriétaires, des exploitants ou du personnel de maintenance. En outre, les signatures électroniques ne devraient être utilisées que pour répondre aux besoins de maintenance et aux besoins opérationnels liés à la présente CC. Les signatures électroniques ne peuvent être considérées comme acceptables dans d'autres domaines couverts par CFR 14 qui ont une applicabilité plus spécifique (c'est-à-dire des dépositions et diverses autres applications). L'acceptation de signatures électroniques encouragera l'utilisation de systèmes électroniques de gestion de documents, mais la FAA continue d'accepter les documents papier pour répondre aux besoins réglementaires en vigueur.
-

Appendice 2 au Chapitre 5

DESCRIPTION DE POSTE TYPE POUR UN DIRECTEUR DE LA SÉCURITÉ

1. FONCTION GÉNÉRALE

Le directeur de la sécurité est responsable devant le Dirigeant responsable de la fourniture d'avis et de stratégies pour la planification, la mise en œuvre et le fonctionnement du système de gestion de la sécurité de l'organisation (SGS). Le directeur de la sécurité fournit des services liés au SGS aux secteurs certifiés, non certifiés et tiers secteurs de l'organisation qui sont inclus dans le SGS et peut avoir des responsabilités qui lui sont déléguées au nom de personnes titulaires de postes requis par les règlements.

2. RÔLES CLÉS

Défenseur de la sécurité

- Démonstre un comportement et une attitude excellents, suit les pratiques et les règles réglementaires, reconnaît les dangers et en rend compte et promeut des comptes rendus de sécurité efficaces.

Leader

- Par un leadership effectif, façonne et promeut une culture organisationnelle qui encourage les pratiques de sécurité.

Communicateur

- Agit comme canal d'information pour porter les questions de sécurité à l'attention de la direction et communiquer cette information au personnel, aux sous-traitants et aux parties prenantes de l'organisation.
- Fournit et articule l'information concernant les questions de sécurité au sein de l'organisation.

Développeur

- Contribue à l'amélioration continue des dispositifs d'identification des dangers et d'évaluation des risques de sécurité et à l'amélioration du SGS de l'organisation.

Bâtisseur de relations

- Édifie et entretient d'excellentes relations de travail avec le Groupe d'action pour la sécurité (GAS) et le bureau des services de sécurité (BSS) de l'organisation.

Ambassadeur

- Représente l'organisation auprès des instances gouvernementales, internationales et de l'industrie (par exemple OACI, IATA, AAC, AIB, etc.).

Analyste

- Analyse les données techniques à la recherche des tendances relatives aux dangers, événements et occurrences.

Gestionnaire de processus

- Utilise efficacement les processus et procédures applicables pour s'acquitter de ses rôles et responsabilités.
- Étudie les possibilités d'accroître l'efficacité des processus.
- Mesure l'efficacité et cherche à accroître constamment la qualité des processus.

3. RESPONSABILITÉS

Entre autres fonctions, le directeur de la sécurité est chargé :

- de la gestion du fonctionnement du système de gestion de la sécurité ;
- de la collecte et de l'analyse des renseignements sur la sécurité, en temps opportun ;
- de l'administration des enquêtes liées à la sécurité ;
- de la surveillance et de l'évaluation des résultats des mesures correctrices ;
- de veiller à ce que des évaluations de risques soient menées lorsqu'il le faut ;
- de la surveillance de l'industrie, s'agissant de problèmes de sécurité qui pourraient toucher l'organisation ;
- de participer à des interventions d'urgence réelles ou d'entraînements ;
- de participer à l'élaboration et à l'actualisation du plan et des procédures d'intervention d'urgence ;
- de veiller à ce que les renseignements liés à la sécurité, y compris les buts et objectifs de l'organisation, soient communiqués à tout le personnel selon les processus de communication établis.

4. NATURE ET PORTÉE

Le directeur de la sécurité devra interagir avec le personnel opérationnel, les cadres supérieurs et les chefs de service dans toute l'organisation. Il devrait aussi entretenir des relations positives avec les autorités de réglementation, agences et prestataires de produits et services à l'extérieur de l'organisation. D'autres contacts de travail seront établis selon les besoins.

5. QUALIFICATIONS

Le directeur de la sécurité devrait avoir les qualifications suivantes :

- une expérience à temps complet de la sécurité de l'aviation, en qualité d'enquêteur sur la sécurité de l'aviation, de gestionnaire de la sécurité/qualité ou de gestionnaire des risques de sécurité ;
- une bonne connaissance des opérations, des procédures et activités de l'organisation ;
- de vastes connaissances techniques en aviation ;
- une connaissance étendue des systèmes de gestion de la sécurité (SGS) et avoir achevé une formation appropriée au SGS ;
- une compréhension des principes et techniques de la gestion des risques, afin d'appuyer le SGS ;
- une expérience de la mise en œuvre et/ou de la gestion d'un SGS ;
- l'expérience et des qualifications dans les enquêtes sur les accidents/incidents d'aviation et les facteurs humains ;
- une expérience et des qualifications de la conduite d'audits et d'inspections de la sécurité/qualité ;
- des connaissances solides des cadres réglementaires de l'aviation, et notamment les normes et pratiques recommandées de l'OACI (SARP) et des règlements pertinents de l'aviation civile ;
- l'aptitude à établir des relations à tous les niveaux, à l'intérieur et à l'extérieur de l'organisation ;
- l'aptitude à être ferme dans ses convictions, à favoriser une « culture d'équité et de justice » tout en installant une atmosphère ouverte et non punitive de comptes rendus ;
- l'aptitude et la confiance nécessaires pour communiquer directement avec le Dirigeant responsable en qualité de conseiller et de confident ;
- de bonnes capacités de communication et des compétences interpersonnelles élevées, lui permettant d'assurer la liaison avec toute une gamme de personnes et de représentants d'organisations, y compris ceux qui viennent de milieux culturels différents ;
- des connaissances en informatique et de bonnes capacités d'analyse.

6. POUVOIRS

6.1 En ce qui concerne les questions de sécurité, le directeur de la sécurité a directement accès au Dirigeant responsable ainsi qu'à la haute direction et aux cadres supérieurs et moyens appropriés.

6.2 Le directeur de la sécurité est autorisé, sous la direction du Dirigeant responsable, à procéder à des audits, enquêtes et inspections de sécurité de tout aspect des opérations, conformément aux procédures spécifiées dans la documentation relative au système de gestion de la sécurité.

6.3 Le directeur de la sécurité a le pouvoir, sous la direction du Dirigeant responsable, de procéder à des investigations sur des événements de sécurité interne, conformément aux procédures spécifiées dans la documentation relative au SGS de l'organisation.

6.4 Le directeur de la sécurité ne devrait pas détenir d'autres postes ou responsabilités qui pourraient entrer en conflit avec son rôle de directeur de la sécurité du SGS ou y porter atteinte. Son poste devrait faire partie de la haute direction et ne pas être de rang inférieur aux fonctions de production ou opérationnelles de l'organisation.

Appendice 3 au Chapitre 5

PLANIFICATION DES INTERVENTIONS D'URGENCE

1. C'est peut-être parce que les accidents d'aviation sont rares que peu d'organisations sont prêtes pour y faire face. Beaucoup d'organisations n'ont pas mis en place de plans efficaces pour gérer les événements pendant ou après une situation d'urgence ou une crise. Or, la façon dont une organisation s'en sort après un accident ou une autre situation d'urgence peut dépendre de la qualité de sa gestion des premières heures ou des premiers jours suivant un grave événement lié à la sécurité. Un plan d'intervention d'urgence (ERP) énonce par écrit ce qu'il faut faire après un accident et qui est responsable de chaque action. Chez les divers prestataires de produits et de services, un tel plan est désigné par des termes différents comme plan d'urgence, plan de gestion de crise et plan de soutien au maintien de la navigabilité. Dans le présent manuel, le terme générique Plan d'intervention d'urgence (ERP) est utilisé pour désigner les plans d'urgence pertinents attendus des prestataires de services d'aviation dont les produits/services peuvent avoir une incidence sur la sécurité de l'aviation.

2. S'il est normal d'associer la planification des interventions d'urgence aux opérations aériennes et aéroportuaires, généralement dans le cas d'un accident d'aéronef, le concept peut également s'appliquer à d'autres prestataires de services. Dans le cas des fournisseurs de services ATS, il peut s'agir de faire face à une importante coupure de courant, à une perte de couverture radar, à une défaillance des communications ou d'autres installations majeures. Pour un organisme de maintenance, il peut s'agir d'une violation grave des exigences en matière de navigabilité, entraînant l'immobilisation au sol d'une flotte (AOG). Pour un organisme de conception et de fabrication, une défaillance grave de conception peut aboutir à une immobilisation au sol générale qui appelle d'urgence une nouvelle conception, la modification, la production et la conversion (directive de navigabilité d'urgence) pour régler une telle crise. Lorsqu'il est possible que les opérations ou activités d'aviation d'un organisme soient compromises par d'autres crises ou urgences provenant de sources externes, comme une urgence sanitaire publique ou une pandémie publique, ces scénarios devraient être également traités dans son ERP d'aviation, selon les besoins. Ainsi, un ERP est essentiellement une composante intégrale de la procédure de gestion des risques de sûreté d'une organisation pour traiter toutes les situations d'urgence, crises ou événements possibles liés à la sécurité ou à la qualité, auxquels ses produits ou services pourraient contribuer ou être associés. L'ERP devrait traiter tous les scénarios possibles/vraisemblables et comprendre des mesures ou procédés d'atténuation appropriés pour que l'organisation, ses clients, le public et/ou l'industrie dans son ensemble puissent avoir un meilleur niveau d'assurance de sécurité ainsi qu'une meilleure continuité de service.

3. Une gestion réussie d'un cas d'urgence commence par une planification efficace. Un ERP fournit la base d'une approche systématique de la gestion des activités de l'organisation à la suite d'un événement imprévu important qui, dans le pire des cas, peut être un accident grave.

4. L'objet d'un Plan d'intervention d'urgence (ERP) est de prévoir :

- a) la délégation des pouvoirs d'urgence ;
- b) l'attribution des responsabilités d'urgence ;
- c) la documentation relative aux procédures et procédés d'urgence ;
- d) la coordination des efforts d'urgence à l'interne et avec les parties externes ;

- e) la poursuite en toute sécurité des opérations essentielles, pendant la gestion de la crise ;
 - f) l'identification proactive de tous les événements/scénarios d'urgence possibles et de leurs mesures d'atténuation correspondantes, etc.
5. Pour être efficace, un ERP devrait :
- a) être adapté à la taille, à la nature et à la complexité de l'organisation ;
 - b) être facilement accessible pour tout le personnel pertinent et les autres organisations, au besoin ;
 - c) inclure des listes de vérification et procédures pertinentes à des situations d'urgence spécifiques ;
 - d) comprendre les coordonnées détaillées du personnel pertinent afin de le contacter rapidement ;
 - e) être testé régulièrement au moyen d'exercices ;
 - f) être revu périodiquement et actualisé lors du changement de certains détails, etc.

Contenu d'un ERP

6. L'ERP sera normalement présenté sous la forme d'un manuel. Il devrait exposer les responsabilités, rôles et actions des divers organismes et personnels qui devront gérer des situations d'urgence précises. L'ERP devrait tenir compte de considérations telles que les suivantes :
- a) *Politiques en vigueur.* L'ERP devrait donner des directives concernant les interventions en cas d'urgence, notamment lois et réglementations régissant les enquêtes, accords passés avec les autorités locales, politiques de la compagnie et ses priorités.
 - b) *Organisation.* L'ERP devrait décrire les intentions de la direction en ce qui concerne les organismes appelés à intervenir :
 - 1) en désignant qui sera affecté aux équipes d'intervention et en spécifiant qui les dirigera ;
 - 2) en définissant les rôles et responsabilités du personnel affecté aux équipes d'intervention ;
 - 3) en clarifiant les liens hiérarchiques ;
 - 4) en mettant sur pied d'un centre de gestion des crises (CMC) ;
 - 5) en instaurant des procédures pour la réception d'un grand nombre de demandes d'informations, surtout pendant les premiers jours suivant un grave accident ;
 - 6) en désignant le porte-parole de la compagnie qui assurera le contact avec les médias ;
 - 7) en définissant les ressources qui seront disponibles, y compris les autorisations financières pour les activités immédiates ;
 - 8) en désignant le représentant de la compagnie pour toute enquête officielle qui serait entreprise par des agents de l'État ;

- 9) en définissant un plan de rappel au travail du personnel clé, etc.

Un organigramme pourrait être utilisé pour montrer les fonctions au sein de l'organisation et les flux de communications entre ces fonctions.

- c) *Notifications.* Le plan devrait spécifier quelles personnes au sein de l'organisation il faut avertir d'une situation d'urgence, qui en enverra notification à l'extérieur et par quels moyens. Il faudrait envisager de signaler l'événement aux personnes ci-dessous :
 - 1) la direction ;
 - 2) les autorités nationales (services de recherche et de sauvetage, autorité de réglementation, bureau d'enquêtes sur les accidents, etc.) ;
 - 3) les services locaux d'intervention en cas d'urgence (autorités aéroportuaires, pompiers, police, services d'ambulance, organismes médicaux, etc.) ;
 - 4) les proches des victimes (une question sensible qui est gérée par la police dans de nombreux États) ;
 - 5) le personnel de la compagnie ;
 - 6) les médias ;
 - 7) les représentants légaux, les mandataires comptables, assureurs, etc.
- d) *Première intervention.* En fonction des circonstances, une équipe de première intervention peut être envoyée sur le site de la crise ou de l'accident pour renforcer les ressources locales et surveiller les intérêts de l'organisation. Voici quelques facteurs à envisager lors de la constitution d'une équipe de première intervention :
 - 1) Qui devrait diriger l'équipe de première intervention ?
 - 2) Qui devrait faire partie de l'équipe de première intervention ?
 - 3) Qui devrait parler au nom de l'organisation sur le site de l'accident ?
 - 4) Quels seraient les besoins en termes d'équipements spéciaux, de vêtements, de documentation, de moyens de transport, d'hébergement, etc. ?
- e) *Aide supplémentaire.* Des membres du personnel ayant la formation et l'expérience appropriées peuvent offrir un soutien utile pendant l'élaboration, les exercices et la mise à jour de l'ERP de l'organisation. Leur savoir-faire peut être utile pour planifier et exécuter des tâches telles que :
 - 1) tenir le rôle de passagers ou de clients dans des exercices de secours ;
 - 2) aider les survivants ;
 - 3) gérer le contact avec les familles des victimes.

f) *Centre de gestion des crises (CMC)*. Un CMC (normalement en état de veille) pourra être installé au siège de l'organisation lorsque la situation répond aux critères d'activation. En outre, un poste de commandement peut être installé sur le site de la crise ou à proximité de ce site. L'ERP devrait préciser comment l'organisation répondra aux besoins en termes de :

- 1) dotation en personnel (éventuellement pour un service assuré 24 heures sur 24, 7 jours sur 7, pendant la période de première intervention) ;
- 2) équipements de communication (téléphones, fax, Internet, etc.) ;
- 3) documentation, tenue des registres des activités d'intervention ;
- 4) saisie des dossiers de la compagnie qui concernent la situation d'urgence ;
- 5) mobilier et fournitures de bureau ;
- 6) documents de référence (tels que les listes de vérification et procédures d'intervention en cas d'urgence, manuels de la compagnie, plans d'urgence d'aérodrome et listes de numéros de téléphone).

Il se peut que l'exploitant, qu'il s'agisse d'une compagnie aérienne ou d'une autre organisation spécialisée, doive sous-traiter les services d'un centre de crise pour veiller à ses intérêts lorsque la situation d'urgence s'est produite loin de l'aéroport d'attache. Du personnel de la compagnie viendrait normalement renforcer dès que possible le centre assurant le service en sous-traitance.

g) *Dossiers*. Non seulement l'organisation doit tenir à jour des registres des événements et activités, mais elle sera aussi tenue de fournir des informations à l'équipe d'enquête de l'État. L'ERP devrait prévoir que les types d'informations suivantes soient mis à la disposition des enquêteurs :

- 1) tous les dossiers pertinents concernant le produit ou service concerné, etc. ;
- 2) des listes de points de contact et de tous les membres du personnel associés à l'événement ;
- 3) les notes prises lors des entrevues avec des personnes associées à l'événement et les déclarations de ces personnes ;
- 4) les preuves photographiques ou autres.

h) *Site de l'accident*. Après un accident grave, des représentants de nombreuses autorités ont des raisons légitimes d'accéder au site, notamment la police, les pompiers, le corps médical, les autorités aéroportuaires, les médecins légistes, pour s'occuper des victimes, les enquêteurs de l'État, les organismes de secours (par exemple la Croix-Rouge) et même les médias. Bien que la coordination des activités de ces intervenants relève de la responsabilité de la police de l'État et/ou de l'autorité en charge de l'enquête, le prestataire de services devrait clarifier certains aspects des activités sur le site de l'accident. Il devrait prévoir :

- 1) la nomination d'un représentant de haut niveau de la compagnie sur le site de l'accident, que celui-ci soit survenu ;
 - à l'aéroport d'attache ;

- loin de l'aéroport d'attache ;
 - en mer ou à l'étranger ;
 - 2) la gestion des passagers survivants ;
 - 3) comment répondre aux besoins des proches des victimes ;
 - 4) la sécurisation de l'épave ;
 - 5) le traitement des restes humains et des objets personnels des défunts ;
 - 6) comment préserver les preuves ;
 - 7) la fourniture d'assistance aux autorités d'enquête (le cas échéant) ;
 - 8) comment enlever et éliminer l'épave, etc.
- i) *Médias d'information.* La réaction de la compagnie vis-à-vis des médias peut avoir une incidence sur la façon dont elle se remettra de l'événement. Des instructions claires sont nécessaires en ce qui concerne, entre autres :
- 1) les informations protégées par la loi (données de l'enregistreur de données de vol [FDR], enregistrements de l'enregistreur de conversations du poste de pilotage [CVR] et enregistrements ATC, déclarations de témoins, etc.) ;
 - 2) la personne habilitée à s'exprimer au nom de l'organisation parente, tant au siège que sur le site de l'accident (directeur des relations publiques, directeur général ou autre cadre supérieur, directeur ou propriétaire) ;
 - 3) une déclaration préparée pour répondre immédiatement aux questions des médias ;
 - 4) les informations qui peuvent ou ne peuvent pas être divulguées ;
 - 5) le choix du moment et du contenu de la première déclaration de la compagnie ;
 - 6) la fourniture de mises à jour régulières aux médias.
- j) *Enquêtes officielles.* Des indications pour le personnel de la compagnie qui entrera en contact avec les enquêteurs de l'État et la police devraient être fournies dans l'ERP.
- k) *Aide aux familles.* L'ERP devrait aussi comporter des éléments indicatifs sur la façon dont la compagnie aidera les familles des victimes de l'accident ou les associations de clients. Ces indications pourraient couvrir des matières telles que :
- 1) les exigences de l'État concernant la fourniture de services d'aide ;
 - 2) les dispositions relatives aux déplacements et à l'hébergement pour visiter le lieu de l'accident ;
 - 3) la désignation d'un coordonnateur du programme et d'un ou plusieurs points de contact pour les victimes ou les clients ;

- 4) la fourniture d'informations actualisées ;
- 5) l'assistance temporaire aux victimes ou aux clients.

Note.— La Circulaire 285 de l'OACI, Éléments d'orientations sur l'assistance aux victimes d'accidents d'aviation et à leurs familles, fournit d'autres orientations sur cette question.

- l) *Évaluation après l'occurrence.* Des indications devraient être données pour garantir que, à la suite de la situation d'urgence, le personnel clé effectue un débriefing complet et consigne toutes les leçons importantes tirées de cette occurrence, ce qui pourrait amener à apporter des modifications à l'ERP et aux procédures associées.

Listes de vérification

7. Toute personne participant à la première intervention à la suite d'un grave accident d'aviation subira un certain choc. C'est pourquoi le processus d'intervention d'urgence se prête à l'utilisation de listes de vérification. Celles-ci peuvent faire partie intégrante des manuels d'exploitation ou d'intervention d'urgence de la compagnie. Pour être efficaces, les listes de vérification doivent être régulièrement :

- a) revues et mises à jour (listes de rappel et coordonnées de contact, par exemple) ;
- b) testées au cours d'exercices réalistes.

Formation et exercices

8. Un plan d'intervention d'urgence est une déclaration d'intention écrite. Il est à espérer qu'une grande partie de l'ERP ne sera jamais testée en conditions réelles. Dès lors, une formation est nécessaire pour assurer que les intentions énoncées dans l'ERP sont soutenues par des capacités opérationnelles. La formation n'ayant qu'une courte « durée utile », il est à conseiller de prévoir des exercices et entraînements réguliers. Certaines parties de l'ERP, telles que les plans de rappel et de communication, peuvent être testées au moyen d'exercices « sur table ». D'autres aspects, tels que les activités « sur site » auxquelles participent d'autres organismes, doivent faire l'objet d'exercices réguliers. La tenue d'exercices présente l'avantage de révéler les lacunes du plan, qui pourront être corrigées avant que ne se produise une réelle situation d'urgence. Pour certains prestataires de services comme les aéroports, la mise à l'essai régulière de l'adéquation du plan et la tenue d'un exercice d'urgence à pleine échelle peuvent être obligatoires.

Appendice 4 au Chapitre 5

ORIENTATIONS SUR L'ÉLABORATION D'UN MANUEL SGS

1. GÉNÉRALITÉS

1.1 Le présent appendice est destiné à guider les organisations dans leur élaboration d'un manuel (ou document) SGS de haut niveau pour définir leur cadre SGS et ses éléments associés. Le manuel peut être un manuel SGS indépendant ou une section/chapitre récapitulative concernant le SGS dans un manuel approuvé approprié de l'organisation (par exemple le manuel de présentation d'une entreprise ou le manuel de l'entreprise). La configuration réelle du document pourra dépendre des attentes réglementaires.

1.2 L'utilisation du format et des postes de contenu suggérés dans le présent appendice, après adaptation appropriée, peut être l'une des façons dont une organisation peut élaborer son propre manuel SGS de haut niveau. Les postes effectifs de contenu dépendront du cadre SGS spécifique et des éléments spécifiques de l'organisation. La description figurant sous chaque élément dépendra de l'ampleur et de la complexité des processus SGS de l'organisation.

1.3 Le manuel servira à diffuser à l'interne le cadre SGS de l'organisation et aux organisations externes pertinentes. Le manuel pourra faire l'objet d'un entérinement ou d'une approbation de l'AAC comme preuve de l'acceptation du SGS.

Note.— Il convient de distinguer un manuel SGS des dossiers et documents justificatifs opérationnels concernant le système. Ces derniers s'entendent des dossiers et documents historiques et actuels produits pendant la mise en œuvre et le fonctionnement des divers processus SGS. Il s'agit de preuves documentaires des activités en cours du SGS de l'organisation.

2. FORMAT DU MANUEL SGS

2.1 Le manuel SGS peut être formaté de la manière suivante :

- a) titre de section ;
- b) objectif ;
- c) critères ;
- d) documents de référence.

2.2 En dessous de chaque « titre de section » numéroté figure une description de l'« objectif » de cette section, suivie des « critères » et des « documents de référence ». L'objectif est ce que l'organisation entend réaliser en faisant ce qui est décrit dans la section. Les critères définissent la portée de ce qui devrait être pris en compte lors de la rédaction de cette section. Les documents de référence relient l'information à d'autres manuels ou SOP pertinents de l'organisation qui contiennent des détails de l'élément ou du processus, selon le cas.

3. TENEUR DU MANUEL

3.1 La teneur du manuel peut comprendre les sections suivantes :

1. contrôle des documents ;
2. exigences réglementaires du SGS ;
3. portée et intégration du système de gestion de la sécurité ;
4. politique de sécurité ;
5. objectifs de sécurité ;
6. imputabilité en matière de sécurité et personnel clé ;
7. comptes rendus de sécurité et mesures correctrices ;
8. identification des dangers et évaluation des risques ;
9. surveillance et mesure de la performance de sécurité ;
10. enquêtes liées à la sécurité et mesures correctrices ;
11. formation et communication en matière de sécurité ;
12. amélioration continue et audit du SGS ;
13. gestion des dossiers du SGS ;
14. la gestion du changement ;
15. plan d'intervention d'urgence/en situation d'urgence.

3.2 L'exemple ci-dessous indique le type de renseignements qui pourraient être inclus dans chaque section dans le format prescrit au § 2.2.

1. Contrôle des documents

Objectif

Décrire comment le ou les manuels seront tenus à jour et comment l'organisation veillera à ce que tout le personnel participant à des fonctions liées à la sécurité dispose de la version la plus à jour.

Critères

- a) Exemplaire papier ou support électronique contrôlé et liste de distribution.
- b) Corrélation entre le manuel SGS et d'autres manuels existants comme le manuel du contrôle de maintenance (MCM) ou le manuel d'exploitation.
- c) Le processus d'examens périodiques du manuel et de ses formulaires/documents connexes pour veiller à ce qu'ils soient continuellement adaptés, adéquats et efficaces.
- d) Processus d'administration, d'approbation et d'acceptation réglementaire du manuel.

Documents de référence

Manuel de qualité, manuel technique, etc.

2. Exigences réglementaires du SGS

Objectif

Mentionner les règlements et éléments indicatifs du SGS en vigueur aux fins de référence et de sensibilisation nécessaires de toutes les parties concernées.

Critères

- a) Préciser les règlements/normes en vigueur du SGS. Inclure le calendrier d'application des dispositions et les références des documents d'information, selon le cas.
- b) Selon les besoins, développer ou expliquer l'importance et les incidences des règlements pour l'organisation.
- c) Établir une corrélation avec les autres exigences ou normes de sécurité, selon le cas.

Documents de référence

Références des règlements/spécifications du SGS, références des documents d'orientation du SGS, etc.

3. Portée et intégration du système de gestion de la sécurité

Objectif

Décrire la portée et l'étendue des opérations et installations de l'organisation liées à l'aviation dans lesquelles le SGS s'appliquera. La portée des procédés, de l'équipement et des opérations jugés utiles au programme d'identification des dangers et de gestion des risques (HIRM) de l'organisation devrait être également mentionnée.

Critères

- a) Préciser la nature des affaires d'aviation de l'organisation et sa position ou son rôle dans l'industrie dans son ensemble.
- b) Identifier les domaines, services, ateliers et installations principaux de l'organisation dans lesquels le SGS s'appliquera.
- c) Identifier les processus, opérations et équipements majeurs qui sont jugés utiles pour le programme HIRM de l'organisation, en particulier ceux qui sont pertinents à la sécurité de l'aviation. Si la portée des processus, opérations et équipements jugés utiles pour le HIRM est trop détaillée ou trop longue, elle peut faire l'objet d'un document complémentaire, au besoin.
- d) Lorsqu'on attend du SGS qu'il fonctionne ou soit administré pour un groupe d'organisations ou de sous-traitants interreliés, définir et documenter cette intégration et ses imputabilités associées, selon le cas.
- e) Lorsqu'il y a d'autres systèmes de contrôle/gestion connexes dans l'organisation, comme le SGQ, l'OSHE et le SeMS, préciser leur intégration pertinente (selon le cas) dans le SGS aviation.

Documents de référence

Manuel de qualité, manuel technique, etc.

4. Politique de sécurité*Objectif*

Décrire les intentions, les principes de gestion et l'engagement de l'organisation, d'améliorer la sécurité de l'aviation en termes de produits ou de prestataire de services. Une politique de sécurité devrait être une brève description, analogue à un énoncé de mission.

Critères

- a) La politique de sécurité devrait correspondre à la taille et à la complexité de l'organisation.
- b) La politique de sécurité énonce les intentions, les principes de gestion et l'engagement de l'organisation d'améliorer constamment la sécurité de l'aviation.
- c) La politique de sécurité est approuvée et signée par le Dirigeant responsable.
- d) La politique de sécurité est promue par le Dirigeant responsable et tous les autres dirigeants.
- e) La politique de sécurité est revue périodiquement.
- f) Le personnel, à tous les niveaux, participe à l'établissement et à la maintenance du système de gestion de la sécurité.
- g) La politique de sécurité est communiquée à tous les employés, afin de les sensibiliser à leurs obligations individuelles en matière de sécurité.

Documents de référence

Politique de sécurité OSHE, etc.

5. Objectifs de sécurité*Objectif*

Décrire les objectifs de sécurité de l'organisation. Les objectifs de sécurité devraient être une brève déclaration qui décrit en termes larges ce que l'organisation espère réaliser.

Critères

- a) Les objectifs de sécurité ont été établis.
- b) Les objectifs de sécurité sont exprimés en tant que déclaration de haut niveau décrivant l'engagement de l'organisation de réaliser la sécurité.
- c) Il y a un processus formel d'élaboration d'un ensemble cohérent d'objectifs de sécurité.

- d) Les objectifs de sécurité sont médiatisés et diffusés.
- e) Les ressources ont été affectées en vue de la réalisation des objectifs.
- f) Les objectifs de sécurité sont liés à des indicateurs de sécurité afin de faciliter la surveillance et la mesure, selon le cas.

Documents de référence

Document sur les indicateurs de performance de sécurité, etc.

6. Rôles et responsabilités

Objectif

Décrire les pouvoirs, responsabilités et imputabilités en matière de sécurité du personnel qui participe au SGS.

Critères

- a) Le Dirigeant responsable est chargé de veiller à ce que le système de gestion de la sécurité soit correctement mis en œuvre et qu'il fonctionne conformément aux exigences dans tous les secteurs de l'organisation.
- b) Selon le cas, un directeur de la sécurité (bureau) ou un comité de la sécurité appropriés, ou des groupes d'action pour la sécurité ont été nommés.
- c) Les pouvoirs, les responsabilités et les imputabilités en matière de sécurité du personnel à tous les niveaux de l'organisation sont définis et documentés.
- d) Tout le personnel comprend ses pouvoirs, responsabilités et imputabilités en ce qui concerne tous les processus, décisions et mesures de gestion de la sécurité.
- e) Un diagramme des imputabilités organisationnelles du SGS est disponible.

Documents de référence

Manuel de présentation de l'entreprise, manuel SOP, manuel d'administration, etc.

7. Comptes rendus de sécurité

Objectif

Un système de comptes rendus devrait comprendre à la fois des éléments réactifs (comptes rendus d'accidents/incidents, etc.) et proactifs/prédictifs (comptes rendus de dangers). Décrire les systèmes de comptes rendus respectifs. Les facteurs à prendre en compte comprennent : le format du compte rendu, la confidentialité, les destinataires, les procédures d'investigation/évaluation, les mesures correctrices/préventives et la diffusion du compte rendu.

Critères

- a) L'organisation a une procédure permettant de capter les événements internes, y compris les accidents, incidents et autres événements pertinents au SGS.
- b) Il convient de distinguer entre les comptes rendus obligatoires (accidents, incidents graves, principales défaillances, etc.), qui doivent être notifiés à l'AAC, et les autres comptes rendus d'événements courants, qui demeurent à l'intérieur de l'organisation.
- c) Il y a également un système de comptes rendus volontaires et confidentiels de dangers/événements, intégrant une protection appropriée de l'identité/données, selon le cas.
- d) Les processus de comptes rendus respectifs sont simples, accessibles et correspondent à la taille de l'organisation.
- e) Les comptes rendus à hautes conséquences et les recommandations associées sont transmis au niveau approprié de la direction et examinés par celle-ci.
- f) Les comptes rendus sont rassemblés dans une base de données appropriée afin de faciliter l'analyse nécessaire.

Documents de référence

8. Identification des dangers et évaluation des risques*Objectif*

Décrire le système d'identification des dangers et comment ces données sont rassemblées. Décrire le processus de catégorisation des dangers/risques et leur priorisation ultérieure pour une évaluation de sécurité documentée. Décrire comment le processus d'évaluation de la sécurité est mené et comment les plans de mesures préventives sont mis en œuvre.

Critères

- a) Les dangers identifiés sont évalués, priorisés et traités en vue de l'évaluation des risques, selon les besoins.
- b) Il y a un processus structuré d'évaluation des risques comprenant l'évaluation de la gravité, de la probabilité, de la tolérabilité et des contrôles préventifs.
- c) Les procédures d'identification des dangers et d'évaluation des risques portent essentiellement sur la sécurité de l'aviation, qui est leur contexte fondamental.
- d) Le processus d'évaluation des risques utilise des tableurs, des formulaires ou des logiciels appropriés à la complexité de l'organisation et des opérations en cause.
- e) Les évaluations de la sécurité achevées sont approuvées par le niveau approprié de direction.

- f) Il y a un processus pour évaluer l'efficacité des mesures correctrices, préventives et de rétablissement qui ont été élaborées.
- g) Il y a un processus d'examens périodiques des évaluations de la sécurité achevées et de documentation de leurs résultats.

Documents de référence

9. Surveillance et mesure de la performance de sécurité

Objectif

Décrire le composant surveillance et mesure de la performance de sécurité du SGS. Cela comprend les indicateurs de performance de sécurité du SGS de l'organisation (SPI).

Critères

- a) Le processus formel d'élaboration et de tenue à jour d'un ensemble d'indicateurs de performance de sécurité et leurs cibles de performance associées.
- b) La corrélation est établie entre les SPI et les objectifs de l'organisation, selon le cas, et le processus d'acceptation réglementaire des SPI, s'il y a lieu.
- c) Le processus de surveillance de la performance de ces SPI et notamment la procédure de mesures correctrices toutes les fois que des tendances inacceptables ou anormales sont déclenchées.
- d) Tout autre critère ou processus complémentaire du SGS ou pour la surveillance et la mesure de la performance de sécurité.

Documents de référence

10. Investigations et mesures correctrices liées à la sécurité

Objectif

Décrire comment se font les enquêtes et le traitement des accidents/incidents/événements au sein de l'organisation, et notamment leur corrélation avec le système d'identification des dangers et de gestion des risques du SGS de l'organisation.

Critères

- a) Il y a des procédures pour veiller à ce que les accidents et incidents signalés fassent l'objet d'une enquête interne.
- b) Diffusion à l'interne des rapports d'investigations achevés ainsi qu'à l'AAC, s'il y a lieu.

- c) Un processus pour que les mesures correctrices prises ou recommandées soient exécutées et pour l'évaluation de leurs résultats/efficacité.
- d) Une procédure d'enquête disciplinaire est en place, ainsi que des mesures associées aux résultats des investigations.
- e) Des conditions clairement définies dans lesquelles une mesure disciplinaire punitive serait envisagée (par exemple activité illégale, négligence, négligence grave ou faute intentionnelle).
- f) Un processus pour veiller à ce que les investigations comprennent l'identification des défaillances actives ainsi que des facteurs et dangers contributifs.
- g) La procédure et le format des investigations prévoient que les constatations relatives aux facteurs ou dangers contributifs soient traitées en vue de mesures de suivi par le système d'identification des dangers et de gestion des risques de l'organisation, s'il y a lieu.

Documents de référence

11. Formation et communication en matière de sécurité

Objectif

Décrire le type de formation au SGS et autre formation liée à la sécurité que le personnel reçoit et le processus permettant de vérifier l'efficacité de la formation. Décrire comment ces procédures de formation sont documentées. Décrire les processus/voies de communication de sécurité au sein de l'organisation.

Critères

- a) Le programme de formation, les conditions d'admission et les exigences sont documentés.
- b) Il y a un processus de validation qui mesure l'efficacité de la formation.
- c) La formation comprend la formation initiale, la formation périodique et la formation de recyclage, selon le cas.
- d) La formation au SGS de l'organisation fait partie du programme global de formation de l'organisation.
- e) La sensibilisation au SGS est intégrée dans le programme d'emploi ou de familiarisation.
- f) Les processus/voies de communication de sécurité au sein de l'organisation.

Documents de référence

12. Amélioration continue et audit du SGS

Objectif

Décrire le processus de l'examen et de l'amélioration continue du SGS.

Critères

- a) Le processus d'audits et d'examens internes périodiques du SGS de l'organisation afin de veiller à ce qu'il reste constamment adapté, adéquat et efficace.
- b) Décrire tous autres programmes qui contribuent à l'amélioration continue du SGS et de la performance de sécurité de l'organisation, par exemple le MEDA, les enquêtes de sécurité, les systèmes ISO.

Documents de référence

13. Gestion des dossiers du SGS

Objectif

Décrire la méthode de stockage de tous les dossiers et documents liés au SGS.

Critères

- a) L'organisation a un système de dossiers ou d'archivage du SGS qui permet de garder tous les dossiers produits en rapport avec la mise en œuvre et le fonctionnement du SGS.
- b) Les dossiers à conserver comprennent les comptes rendus de dangers, les comptes rendus d'évaluation des risques, les notes des groupes d'action pour la sécurité/réunions de sécurité, les diagrammes des indicateurs de performance de sécurité, les rapports d'audit du SGS et les dossiers de formation au SGS.
- c) Les dossiers devraient permettre de retracer tous les éléments du SGS et être accessibles pour l'administration courante du SGS ainsi qu'aux fins d'audits internes et externes.

Documents de référence

14. Gestion du changement

Objectif

Décrire le processus de l'organisation concernant la gestion des changements qui peuvent avoir une incidence sur les risques de sécurité et comment ces processus sont intégrés dans le SGS.

Critères

- a) Des procédures pour veiller à ce que les changements importants de l'organisation ou dans les opérations tiennent compte de toute répercussion qu'ils peuvent avoir sur les risques actuels de sécurité.
- b) Des procédures pour veiller à ce qu'une évaluation appropriée de sécurité soit effectuée avant l'introduction de nouveaux équipements ou de nouveaux processus qui ont des incidences sur les risques de sécurité.
- c) Des procédures pour l'examen des évaluations actuelles de la sécurité chaque fois qu'il y a des changements du processus ou équipements associés.

Documents de référence

Procédures normalisées d'exploitation de l'entreprise concernant la gestion du changement, etc.

15. Plan d'intervention d'urgence/en situation d'urgence*Objectif*

Décrire les intentions de l'organisation concernant les situations d'urgence et leurs commandes de rétablissement correspondantes, ainsi que l'engagement de l'organisation de traiter ces situations d'urgence. Décrire les grands lignes des rôles et responsabilités du personnel clé. Le plan d'intervention d'urgence peut être un document distinct ou il peut faire partie du manuel SGS.

Critères (selon l'organisation)

- a) L'organisation a un plan d'urgence qui décrit les moindres lignes des rôles et responsabilités en cas d'incident, de crise ou d'accident majeur.
- b) Il y a un processus de notification qui inclut une liste d'appel d'urgence et un processus de mobilisation interne.
- c) L'organisation a des arrangements avec d'autres institutions pour une assistance et la fourniture de services d'urgence, selon le cas.
- d) L'organisation a des procédures de fonctionnement en mode urgence, s'il y a lieu.
- e) Il y a une procédure de supervision du bien-être de toutes les personnes touchées et de notification des proches.
- f) L'organisation a établi des procédures pour le traitement des relations avec les médias et les questions d'assurance.
- g) Il y a des responsabilités définies en matière d'enquêtes sur les accidents au sein de l'organisation.
- h) La nécessité de préserver les preuves, de sécuriser la zone affectée et de comptes rendus obligatoires/nationaux est clairement énoncée.

- i) Il y a une formation à la préparation aux situations d'urgence et à l'intervention en cas d'urgence pour le personnel concerné.
- j) Un plan d'enlèvement d'un aéronef ou d'un équipement hors service a été élaboré par l'organisation en consultation avec les propriétaires d'aéronefs/équipement, les exploitants d'aérodromes ou autres institutions, selon le cas.
- k) Une procédure existe d'enregistrement des activités pendant une intervention d'urgence.

Documents de référence

Manuel ERP, etc.

Appendice 5 au Chapitre 5

SYSTÈMES DE COMPTES RENDUS VOLONTAIRES ET CONFIDENTIELS

[Voir les paragraphes 5.3.42 à 5.3.52 ; 5.3.66 à 5.3.73 ; 5.5.4, Élément 2.1 a)]

Note.— Les orientations ci-dessous sont fondées sur l'exemple d'une organisation intégrée d'exploitant aérien et d'organisme de maintenance. Pour d'autres types d'organisations de prestataires de services, ces éléments indicatifs peuvent être adaptés au besoin.

Le système de comptes rendus volontaires et confidentiels d'une organisation devrait, au minimum, définir :

- a) l'objectif du système de comptes rendus ;

Exemple :

L'objectif principal du système de comptes rendus volontaires et confidentiels de [Nom de l'organisation] est de renforcer la sécurité des activités d'aviation de notre entreprise grâce à la collecte de rapports sur des défaillances de sécurité réelles ou potentielles dont, autrement, il n'aurait pas été rendu compte par d'autres voies. Ces rapports peuvent porter sur des événements, des dangers ou menaces pertinents par rapport à la sécurité de nos activités d'aviation. Ce système n'élimine pas la nécessité de comptes rendus formels d'accidents et d'incidents selon les procédures d'exploitation normalisées de notre entreprise, ni de la communication de comptes rendus d'événements obligatoires aux autorités réglementaires pertinentes.

Le [Nom du système] est un système de comptes rendus volontaires, non punitif et confidentiel d'événements et de dangers, administré par le [Nom du service/bureau]. Il prévoit la communication des comptes rendus volontaires d'événements ou de dangers d'aviation pertinents aux activités d'aviation de notre entreprise, tout en protégeant l'identité de la source.

Note.— Lors de la mise en place de ce système, l'organisation devra décider d'intégrer son système de comptes rendus sur la sécurité, la santé et l'environnement au travail (OSHE) dans son système de comptes rendus sur la sécurité de l'aviation ou de l'en séparer. Cela pourra dépendre des attentes ou des besoins respectifs des autorités aéronautiques et des autorités en matière OSHE. Dans les cas où l'entreprise dispose d'un système de comptes rendus OSHE distinct, cela devrait être dûment souligné dans ce paragraphe afin d'orienter la source, au besoin.

- b) la portée des secteurs/domaines d'aviation couverts par le système ;

Exemple :

Le [Nom du système] couvre, entre autres, les domaines suivants :

- a) l'exploitation technique des vols ;
- b) la maintenance des avions en atelier ;
- c) la maintenance des composantes en atelier ;
- d) la gestion technique des flottes ;
- e) la gestion technique de l'inventaire ;
- f) la planification technique ;
- g) les services techniques ;
- h) les dossiers techniques ;
- i) la maintenance en escale ;
- j) etc.

c) qui peut faire un compte rendu volontaire ;

Exemple :

Si vous appartenez à l'un de ces secteurs ou services opérationnels, vous pouvez contribuer au renforcement de la sécurité de l'aviation au moyen du [Nom du système] en rendant compte d'événements, de dangers ou de menaces pertinents aux activités d'aviation de notre organisation :

- a) les membres de l'équipage de conduite et de l'équipage de cabine ;
- b) les contrôleurs de la circulation aérienne ;
- c) les ingénieurs, techniciens ou mécaniciens d'aéronefs titulaires d'une licence ;
- d) les employés des organismes de maintenance, de conception et de fabrication ;
- e) les opérateurs de services d'escale aux aéroports ;
- f) les employés d'aérodrome ;
- g) le personnel de l'aviation en général ;
- h) etc.

d) quand faire un tel compte rendu ;

Exemple :

Vous devriez faire un compte rendu :

- a) lorsque vous souhaitez que d'autres tirent des enseignements et profitent de l'incident ou du danger mais que vous vous souciez de la protection de votre identité ;
- b) lorsqu'il n'y a pas d'autres procédures ou voies appropriées de comptes rendus ;
- c) lorsque vous avez essayé d'autres procédures ou voies de comptes rendus sans que le problème ait été traité.

e) comment les comptes rendus sont traités ;

Exemple :

Le [Nom du système] insiste particulièrement sur la nécessité de protéger l'identité de la source lors du traitement de tous les comptes rendus. Chaque compte rendu sera lu et validé par le gestionnaire. Le gestionnaire peut contacter la source afin de s'assurer qu'il comprend la nature et les circonstances de l'événement/danger dont il est rendu compte et/ou pour obtenir les informations et éclaircissements supplémentaires nécessaires.

Lorsque le gestionnaire a vérifié que l'information obtenue est complète et cohérente, il va dépersonnaliser l'information et saisir les données dans la base de données de [Nom du système]. Dans le cas où il faut solliciter la contribution d'une tierce partie, seules les données dépersonnalisées seront utilisées.

Le formulaire [Nom du système], avec annotation de la date de retour, sera finalement renvoyé à la source. Le gestionnaire s'efforcera d'achever le traitement dans les dix (10) jours ouvrables si des renseignements supplémentaires ne sont pas nécessaires. Dans les cas où le gestionnaire a besoin de discuter avec la source ou de consulter une tierce partie, un délai supplémentaire peut être nécessaire.

Si le gestionnaire n'est pas au bureau pour une période prolongée, le gestionnaire adjoint peut traiter le compte rendu. Les sources peuvent être assurées que chaque compte rendu de [Nom du système] sera lu et suivi soit par le gestionnaire, soit par le gestionnaire adjoint.

*Partage de l'information de sécurité au sein de la compagnie
et de la communauté aéronautique*

Des comptes rendus et extraits pertinents, dépersonnalisés, peuvent être partagés avec l'entreprise ainsi qu'avec des parties prenantes externes de l'aviation, comme il convient. Cela permettra à tout le personnel et à tous les services concernés au sein de la compagnie ainsi qu'au sein des parties prenantes externes de l'aviation compétentes d'examiner leurs propres opérations et d'appuyer l'amélioration de la sécurité de l'aviation dans son ensemble.

S'il ressort de la teneur d'un compte rendu [Nom du système] qu'il s'agit d'une situation ou d'une condition qui pose une menace immédiate ou urgente pour la sécurité de l'aviation, le compte rendu sera traité en priorité et renvoyé, après dépersonnalisation, aux organismes ou autorités pertinents, dès que possible, afin de leur permettre de prendre les mesures de sécurité nécessaires.

f) contacter le gestionnaire de [Nom du système] ;

Exemple :

N'hésitez pas à appeler le gestionnaire de [Nom du système] pour vous renseigner sur le [Nom du système] ou demander un entretien préliminaire avec le gestionnaire de [Nom du système] avant de faire un compte rendu. Le gestionnaire et le gestionnaire adjoint peuvent être contactés pendant les heures de travail, du lundi au vendredi, aux numéros de téléphone suivants :

Administrateur de [Nom du système]
M. ABC
Tél. :

Administrateur adjoint
M. XYZ
Tél. :

Appendice 6 au Chapitre 5

INDICATEURS DE PERFORMANCE DE SÉCURITÉ DU SGS

1. Les Tableaux 5-A6-1 à 5-A6-4 (exemples d'indicateurs de sécurité) fournissent, à titre illustratif, des exemples d'indicateurs de performance de sécurité (SPI) à l'échelle de l'État et leurs critères d'établissement des niveaux d'alerte et des niveaux cibles correspondants. Les SPI du SGS sont indiqués sur le côté droit des tableaux. Les critères d'établissement des niveaux d'alerte et niveaux cibles correspondants pour chaque indicateur doivent être indiqués comme il est illustré. Les indicateurs de performance de sécurité du plan national de sécurité sur le côté gauche des tableaux sont indiqués afin d'établir la corrélation nécessaire entre les indicateurs de sécurité du SGS et du PNS. Les SPI du SGS devraient être élaborés par les prestataires de produits et de services, en consultation avec leurs organismes de réglementation respectifs nationaux. Leurs SPI proposés devraient correspondre aux indicateurs de sécurité du PNS de l'État, de sorte qu'il faut obtenir l'accord/acceptation nécessaire.

2. Le Tableau 5-A6-5 (exemple d'un diagramme d'indicateurs de performance de sécurité du SGS) est un exemple de diagramme d'indicateurs de performance de sécurité du SGS à hautes conséquences. Dans ce cas, il s'agit du taux d'incidents à signaler/obligatoires d'un exploitant de compagnie aérienne. Le diagramme sur la gauche est la performance de l'année précédente, alors que le diagramme sur la droite représente les actualisations des données en cours de l'année actuelle. La détermination du niveau d'alerte est basée sur les critères de base de mesure de l'écart type en matière de sécurité. La formule dans le tableur Excel est « =STDEVP ». Aux fins du calcul de l'écart type pour le manuel, la formule est :

$$\sigma = \sqrt{\frac{\sum (x - \mu)^2}{N}}$$

dans laquelle « X » est la valeur de chaque point de données, « N » est le nombre de points de données, et « μ » est la valeur moyenne de tous les points de données.

3. La cible fixée est une amélioration souhaitée du pourcentage (dans ce cas 5 %) par rapport aux données moyennes de l'année précédente. Ce diagramme est généré par la fiche de données représentée dans le Tableau 5-A6-6.

4. La fiche de données dans le Tableau 5-A6-6 est utilisée pour générer le diagramme d'indicateurs de performance de sécurité représenté dans le Tableau 5-A6-5. La même fiche de données peut être utilisée pour générer tout autre indicateur de performance de sécurité avec les données appropriées et un amendement de la description des indicateurs de performance de sécurité.

5. Le Tableau 5-A6-7 (exemple d'un résumé des performances du SGS) donne un résumé de tous les indicateurs de sécurité du SGS de l'exploitant, avec leurs résultats respectifs en termes de niveaux d'alerte et de niveaux cibles, annotés. Ce résumé peut être établi à la fin de chaque période de surveillance pour donner un aperçu global de la performance du SGS. Si l'on souhaite une récapitulation plus quantitative de la performance, des points appropriés peuvent être attribués à chaque réponse Oui/Non pour chaque résultat en termes de cibles et d'alertes. Par exemple :

Indicateurs à hautes conséquences :

Niveau d'alerte non violé [Oui (4), Non (0)]

Cible atteinte [Oui (3), Non (0)]

Indicateurs à faibles conséquences :

Niveau d'alerte non violé [Oui (2), Non (0)]

Cible atteinte [Oui (1), Non (0)]

On peut ainsi obtenir un score (ou pourcentage) général pour indiquer la performance de sécurité globale du SGS à la fin de toute période donnée de surveillance.

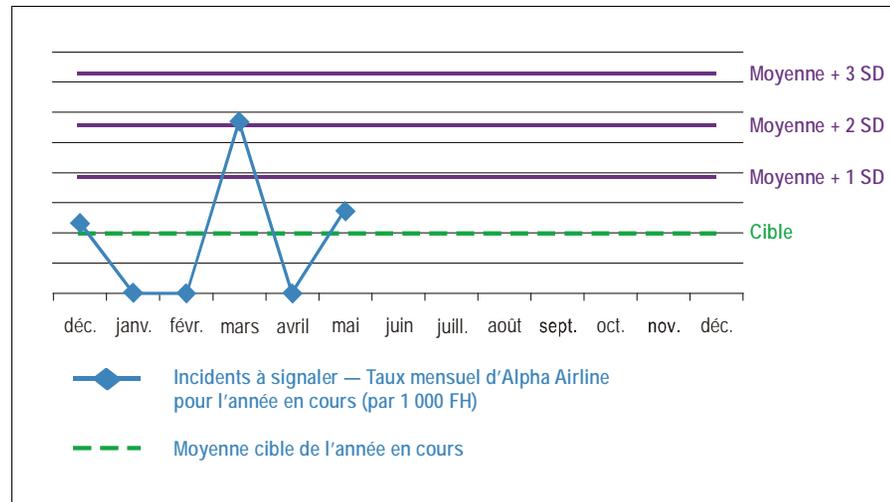
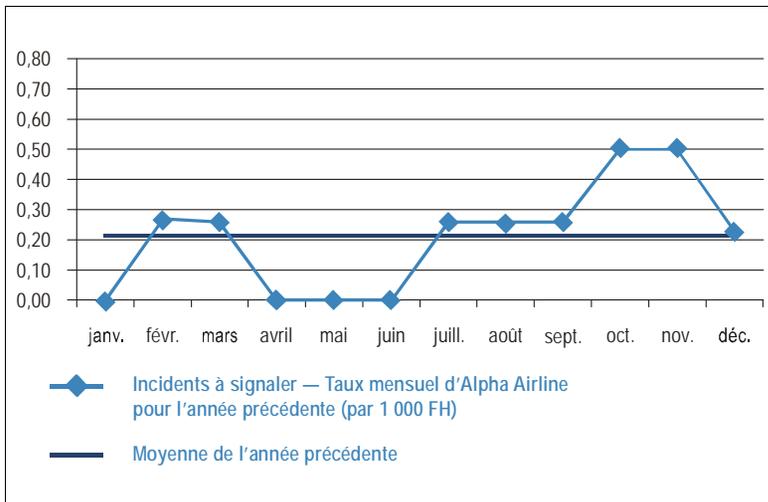
Tableau 5-A6-1. Exemples d'indicateurs de performance de sécurité pour les exploitants aériens

<i>Indicateurs de sécurité figurant dans le PNS (total pour l'État)</i>						<i>Indicateurs de performance de sécurité du SGS (prestataire de services individuel)</i>					
<i>Indicateurs d'événement à hautes conséquences (basés sur l'événement/résultat)</i>			<i>Indicateurs d'événement à faibles conséquences (basés sur l'événement/activité)</i>			<i>Indicateurs d'événement à hautes conséquences (basés sur l'événement/résultat)</i>			<i>Indicateurs d'événement à faibles conséquences (basés sur l'événement/activité)</i>		
<i>Indicateur de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de performance de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>	<i>Indicateur de performance de sécurité</i>	<i>Critères de niveau d'alerte</i>	<i>Critères de niveau cible</i>
Exploitants aériens (de l'État uniquement)											
Taux mensuel /trimestriel d'accidents /d'incidents graves des exploitants aériens de l'AAC (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre	% de LEI ou taux de constatations (constatations par audit) de l'audit annuel de surveillance des exploitants aériens, de l'AAC	A l'étude	A l'étude	Taux mensuel d'incidents graves de la flotte individuelle de l'exploitant aérien (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre	Taux mensuel d'incidents pour la flotte combinée de l'exploitant (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre
Taux trimestriel d'incidents d'arrêt moteur en vol pour les exploitants aériens de l'AAC (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre	% de LEI ou taux de constatations (constatations par inspection) de l'inspection annuelle des stations en ligne, de l'AAC	A l'étude	A l'étude	Taux mensuel d'incidents graves pour la flotte combinée de l'exploitant (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre	% de LEI ou taux de constatations (constatations par audit) de l'audit annuel du SGQ/SGS interne de l'exploitant	A l'étude	A l'étude
			% moyen de LEI (pour chaque exploitant étranger) lors de l'inspection de surveillance des exploitants étrangers sur l'aire de trafic, pour l'AAC	A l'étude	A l'étude	Taux d'incidents d'arrêt moteur en vol de l'exploitant aérien (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre	Taux de comptes rendus volontaires de dangers de l'exploitant (p. ex. par 1 000 FH)	A l'étude	A l'étude
			Taux de comptes rendus d'incidents de marchandises dangereuses concernant les exploitants de l'AAC (p. ex. par 1 000 FH)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre				Taux de comptes rendus d'incidents de marchandises dangereuses concernant l'exploitant	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre
etc.											

Tableau 5-A6-3. Exemples d'indicateurs de performance de sécurité pour les exploitants de services ATS

Indicateurs de sécurité figurant dans le PNS (total pour l'État)						Indicateurs de performance de sécurité du SGS (prestataire individuel de services)					
Indicateurs d'événement à hautes conséquences (basés sur l'événement/résultat)			Indicateurs d'événement à faibles conséquences (basés sur l'événement/activité)			Indicateurs d'événement à hautes conséquences (basés sur l'événement/résultat)			Indicateurs d'événement à faibles conséquences (basés sur l'événement/activité)		
Indicateur de sécurité	Critères de niveau d'alerte	Critères de niveau cible	Indicateur de sécurité	Critères de niveau d'alerte	Critères de niveau cible	Indicateur de performance de sécurité	Critères de niveau d'alerte	Critères de niveau cible	Indicateur de performance de sécurité	Critères de niveau d'alerte	Critères de niveau cible
Exploitants de services ATS											
À l'échelle de l'AAC, taux trimestriel d'incidents ATS graves dans la FIR (espace aérien) — mettant en cause n'importe quel aéronef (p. ex. par 100 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre	Pour l'ensemble des services ATS de l'AAC, taux trimestriel d'incidents avec RA TCAS dans la FIR — mettant en cause n'importe quel aéronef (p. ex. par 100 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre	Taux trimestriel d'incidents graves des services ATS dans la FIR — mettant en cause n'importe quel aéronef (p. ex. par 100 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre	Taux trimestriel d'incidents des services ATS avec RA TCAS dans la FIR— mettant en cause n'importe quel aéronef (p. ex. par 100 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre
			Pour l'ensemble des services ATS de l'AAC, taux trimestriel d'incidents avec perte de séparation dans la FIR — mettant en cause n'importe quel aéronef (p. ex. par 100 000 mouvements aériens) (données AAC)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre	Taux trimestriel/ annuel d'incidents de quasi-collision de l'exploitant de services ATS (p. ex. par 100 000 mouvements aériens)	Dans l'hypothèse où le taux moyen annuel historique est 3, le taux d'alerte possible pourrait être de 5.	Dans l'hypothèse où le taux moyen annuel historique est 3, le taux d'alerte possible pourrait être de 2.	Taux trimestriel d'incidents des services ATS, avec perte de séparation dans la FIR— mettant en cause n'importe quel aéronef (p. ex. par 100 000 mouvements aériens)	Moyenne + 1/2/3 SD (remise à zéro annuelle ou bisannuelle)	__ % (p. ex. 5 %) d'amélioration d'un taux annuel moyen à l'autre
			Pour l'ensemble des services ATS de l'AAC, % de LEI ou taux de constatations (constatations par audit) des audits annuels de surveillance	A l'étude	A l'étude				% de LEI ou taux de constatations (constatations par audit) lors de l'audit annuel du SGO/SGS interne des services ATS	A l'étude	A l'étude
etc.											

Tableau 5-A6-5. Exemple d'un diagramme d'indicateur de performance de sécurité d'un SGS (avec les réglages d'alerte et de niveau cible)



a) Réglage du niveau d'alerte :

Le niveau d'alerte pour une nouvelle période de surveillance (année en cours) est fondé sur la performance de la période précédente (année précédente), à savoir sa moyenne de points de données et son écart type. Les trois lignes d'alerte sont moyenne + 1SD, moyenne + 2SD et moyenne + 3SD.

b) Seuil de niveau d'alerte :

Une alerte (tendance anormale/inacceptable) est indiquée si l'une quelconque des conditions ci-dessous est remplie pour la période de surveillance en cours (année en cours) :

- 1 point quelconque se situe au-dessus de la ligne 3 SD
- 2 points consécutifs se situent au-dessus de la ligne 2 SD
- 3 points consécutifs se situent au-dessus de la ligne 1 SD.

Lorsqu'une alerte est déclenchée (possibilité d'une situation à hauts risques ou incontrôlable), une action appropriée de suivi est attendue, par exemple une analyse plus approfondie pour déterminer la source et la cause profonde du taux anormal d'incidents et toute action nécessaire pour faire face à la tendance inacceptable.

c) Réglage du niveau cible (amélioration planifiée) :

Le réglage du niveau cible peut être moins structuré que le réglage du niveau d'alerte, par exemple la cible sera que le nouveau taux moyen de la période de surveillance (année en cours) sera par exemple inférieur (ou meilleur) de 5 % que la valeur moyenne de la période précédente.

d) Réalisation de l'objectif :

À la fin de l'année en cours, si le taux moyen pour l'année en cours est inférieur d'au moins 5 % ou plus que le taux moyen de l'année précédente, alors on considère que l'objectif fixé d'une amélioration de 5 % a été réalisé.

e) Niveau d'alerte et niveau cible — période de validité :

Les niveaux d'alerte et niveaux cibles devraient être revus (redéfinis) pour chaque nouvelle période de surveillance, sur la base du taux moyen et de l'écart type de la période précédente, selon le cas.

Tableau 5-A6-6. Fiche technique type utilisée pour produire un diagramme d'indicateurs de sécurité du SGS pour les événements à conséquences majeures (avec les critères d'établissement de l'alerte et de la cible)

Année précédente					Année en cours							
Mois	Nombre total d'FH de la Cie Alpha	Nombre d'incidents à signaler/MOR	Taux d'incident*	Moyenne	Mois	Nombre total d'FH de la Cie Alpha	Nombre d'incidents à signaler/MOR	Taux d'incident*	Année précédente moyenne + 1 SD	Année précédente moyenne + 2 SD	Année précédente moyenne + 3 SD	Moyenne cible année en cours
Janvier	3 992	—	0,00	0,21	Décembre	4 369	1,00	0,23	0,39	0,56	0,73	0,21
Février	3 727	1,00	0,27	0,21	Janvier	4 090	0,00	0,00	0,39	0,56	0,73	0,20
Mars	3 900	1,00	0,26	0,21	Février	3 316	0,00	0,00	0,39	0,56	0,73	0,20
Avril	3 870	—	0,00	0,21	Mars	3 482	2,00	0,57	0,39	0,56	0,73	0,20
Mai	3 976	—	0,00	0,21	Avril	3 549	0,00	0,00	0,39	0,56	0,73	0,20
Juin	3 809	—	0,00	0,21	Mai	3 633	1,00	0,28	0,39	0,56	0,73	0,20
Juillet	3 870	1,00	0,26	0,21	Juin				0,39	0,56	0,73	0,20
Août	3 904	1,00	0,26	0,21	Juillet				0,39	0,56	0,73	0,20
Septembre	3 864	1,00	0,26	0,21	Août				0,39	0,56	0,73	0,20
Octobre	3 973	2,00	0,50	0,21	Septembre				0,39	0,56	0,73	0,20
Novembre	3 955	2,00	0,51	0,21	Octobre				0,39	0,56	0,73	0,20
Décembre	4 369	1,00	0,23	0,21	Novembre				0,39	0,56	0,73	0,20
		Moyenne	0,21		Décembre				0,39	0,56	0,73	0,20
		SD	0,18				Moyenne					
							SD					

Moyenne + 1 SD	Moyenne + 2 SD	Moyenne + 3 SD
0,39	0,56	0,73

La cible de l'année en cours est, par exemple, une amélioration de 5 % du taux moyen par rapport au taux moyen pour l'année précédente, qui est :	0,20
---	------

Les critères d'établissement du niveau d'alerte pour l'année en cours sont fondés sur l'année précédente (Moyenne + 1/2/3 SD).

Taux de calcul (par 1 000 FH).

Tableau 5-A6-7. Exemple de la mesure de la performance de sécurité du SGS de la Compagnie Alpha (par exemple pour l'année 2010)

<i>Indicateur de performance de sécurité à conséquences majeures</i>					
	<i>Description de l'indicateur de performance de sécurité (SPI)</i>	<i>Critères du niveau d'alerte du SPI (pour 2010)</i>	<i>Niveau d'alerte dépassé (Oui/Non)</i>	<i>Critères du niveau d'alerte du SPI (pour 2010)</i>	<i>Objectif réalisé (Oui/Non)</i>
1	Taux mensuel d'incidents graves de la flotte d'A320 de la Compagnie Alpha (par exemple par 1 000 FH)	Moyenne + 1/2/3 SD (réinitialisation annuelle ou bisannuelle)	Oui	Amélioration de <u>5 %</u> du taux moyen de 2010 par rapport au taux moyen de 2009	Non
2	Taux d'incidents d'arrêts moteur en vol de la flotte d'A320 de la Compagnie Alpha (par exemple par 1 000 FH)	Moyenne + 1/2/3 SD (réinitialisation annuelle ou bisannuelle)	Oui	Amélioration de <u>3 %</u> du taux moyen de 2010 par rapport au taux moyen de 2009	Oui
3	etc.				

<i>Indicateurs de sécurité pour événement à conséquences plus faibles</i>					
	<i>Description de l'indicateur de performance de sécurité (SPI)</i>	<i>Critères du niveau d'alerte du SPI (pour 2010)</i>	<i>Niveau d'alerte dépassé (Oui/Non)</i>	<i>Critères du niveau d'alerte du SPI (pour 2010)</i>	<i>Objectif réalisé (Oui/Non)</i>
1	Taux mensuel d'incidents de la flotte combinée de l'exploitant (par exemple par 1 000 FH)	Moyenne + 1/2/3 SD (réinitialisation annuelle ou bisannuelle)	Oui	Amélioration de <u>5 %</u> du taux moyen de 2010 par rapport au taux moyen de 2009	Non
2	Pourcentage de LEI ou taux de constatations (constatations par audit) de l'audit annuel du SGQ interne de l'exploitant	Plus de 25 % en moyenne de LEI ou de toutes constatations de niveau 1 ou plus de 5 constatations de niveau 2 par audit	Oui	Amélioration de <u>5 %</u> du taux moyen de 2010 par rapport au taux moyen de 2009	Oui
3	Taux de comptes rendus volontaires de dangers de l'exploitant (par exemple par 1 000 FH)	À déterminer		À déterminer	
4	Taux de comptes rendus d'incidents de marchandises dangereuses de l'exploitant (par exemple par 1 000 FH)	Moyenne + 1/2/3 SD (réinitialisation annuelle ou bisannuelle)	Non	Amélioration de <u>5 %</u> du taux moyen de 2010 par rapport au taux moyen de 2009	Oui
5	etc.				

Note 1.— Autres indicateurs de processus. À part les indicateurs de niveau de sécurité du SGS ci-dessus, il peut exister d'autres indicateurs du niveau du système au sein de chaque domaine opérationnel d'un organisme. On peut citer par exemple des indicateurs de surveillance spécifiques à un système ou à un processus dans le génie technique, les opérations, le SGQ, etc., ou des indicateurs associés à des programmes fondés sur la performance comme la gestion des risques de fatigue ou la gestion du carburant. Ces indicateurs spécifiques à un processus ou à un système devraient à juste titre être administrés dans le cadre du système de processus concerné. Ils peuvent être considérés comme des indicateurs spécifiques d'un système ou d'un niveau de processus qui s'ajoutent aux indicateurs de performance de sécurité de niveau plus élevé. Ils devraient être traités dans les manuels/SOP du système ou processus respectif, selon le

cas. Néanmoins, les critères de détermination des niveaux d'alerte ou des niveaux cibles pour ces indicateurs devraient de préférence être alignés sur ceux des indicateurs de niveau de performance de sécurité du SGS, le cas échéant.

Note 2.— Sélection des indicateurs et des réglages. La combinaison (ou ensemble) d'indicateurs de sécurité d'événement à conséquences majeures ou à conséquences plus faibles doit être choisie par un organisme selon la portée du système de l'organisme. Pour les indicateurs pour lesquels les critères de définition du niveau d'alerte ou niveau cible suggérés ne sont pas applicables, l'organisme peut envisager des critères de remplacement, selon le cas. L'orientation générale est de définir des alertes et des cibles qui tiennent compte des performances historiques récentes ou actuelles.

Appendice 7 au Chapitre 5

LISTE DE VÉRIFICATION POUR L'ANALYSE DES ÉCARTS ET PLAN DE MISE EN ŒUVRE

1. LISTE INITIALE DE CONTRÔLE POUR L'ANALYSE DES ÉCARTS (TABLEAU 5-A7-1)

1.1 La liste de vérification initiale de l'analyse des écarts du Tableau 5-A7-1 peut être utilisée comme modèle pour effectuer la première étape d'une analyse des écarts du SGS. Ce format, avec ses réponses générales « Oui/Non/En partie » fournira une indication initiale de l'ampleur générale des écarts et donc de la charge de travail globale à laquelle il faut s'attendre. Le questionnaire peut être adapté pour répondre aux besoins de l'organisation et à la nature des produits ou services fournis. Cette information initiale devrait être utile pour aider la haute direction à prévoir l'ampleur de l'effort de mise en œuvre du SGS et donc les ressources à fournir. Cette liste de vérification initiale devra être suivie d'un plan approprié de mise en œuvre, conformément aux Tableaux 5-A7-2 et 5-A7-3.

1.2. La réponse « Oui » indique que pour cette question, les résultats de l'organisation atteignent ou dépassent les attentes. Une réponse « Non » indique une lacune substantielle du système existant en ce qui concerne les attentes pour cette question. Une réponse « En partie » indique qu'une amélioration supplémentaire ou que des travaux de développement sont nécessaires en ce qui concerne un processus existant, afin de répondre aux attentes pour cette question.

Note.— Les références du PNS entre crochets [] renvoient aux éléments indicatifs du présent manuel qui concernent la question de l'analyse des écarts.

Tableau 5-A7-1. Liste de vérification pour l'analyse des écarts

N°	Aspect à analyser ou question appelant une réponse	Réponse	État de mise en œuvre
Composant 1 — POLITIQUE ET OBJECTIFS DE SÉCURITÉ			
Élément 1.1 — Engagement et responsabilité de la direction			
1.1-1	Une politique de sécurité a-t-elle été mise en place ? [5.3.7 à 5.3.15 ; 5.5.3]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.1-2	La politique de sécurité reflète-t-elle des engagements de la direction à l'égard de la gestion de la sécurité ? [5.3.7 à 5.3.15]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.1-3	La politique de sécurité est-elle appropriée à la taille, à la nature et à la complexité de l'organisation ? [5.3.7 à 5.3.15]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question appelant une réponse	Réponse	État de mise en œuvre
1.1-4	La politique de sécurité est-elle pertinente à la sécurité de l'aviation ? [5.3.7 à 5.3.15]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.1-5	La politique de sécurité est-elle signée par le Dirigeant responsable ? [5.3.7 à 5.3.15 ; 5.5.3]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.1-6	La politique de sécurité est-elle communiquée, avec une approbation visible, à travers toute [l'organisation] ? [5.5.3]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.1-7	La politique de sécurité est-elle périodiquement réexaminée pour s'assurer qu'elle demeure pertinente et appropriée à [l'organisation] ? [5.5.3]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 1.2 — Imputabilités en matière de sécurité			
1.2-1	[L'organisation] a-t-elle désigné un Dirigeant responsable qui, indépendamment d'autres fonctions, aura la responsabilité et l'imputabilité ultimes, au nom de [l'organisation], de la mise en œuvre et de la tenue à jour du SGS ? [5.3.16 à 5.3.26 ; 5.5.2]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-2	Le Dirigeant responsable a-t-il pleine compétence sur les ressources financières et humaines nécessaires pour que les opérations autorisées soient réalisées en vertu du certificat d'exploitation ? [5.3.16 à 5.3.26]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-3	Le Dirigeant responsable a-t-il l'autorité finale s'agissant de toutes les activités d'aviation de son organisation ? [5.3.16 à 5.3.26]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-4	[L'organisation] a-t-elle précisé et documenté les obligations redditionnelles de la direction en matière de sécurité ainsi que celles du personnel opérationnel en ce qui concerne le SGS ? [5.3.16 à 5.3.26]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-5	Existe-t-il un comité de la sécurité ou conseil d'examen de la sécurité aux fins d'examiner le SGS et la performance de sécurité ? [5.3.27 à 5.3.33 ; Appendice 4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-6	Le comité de la sécurité est-il présidé par le Dirigeant responsable ou par un adjoint dûment désigné, selon une procédure dûment énoncée dans le manuel SGS ? [5.3.27 à 5.3.33 ; Appendice 4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.2-7	Le comité de la sécurité comprend-il, le cas échéant, des chefs opérationnels ou chefs de département pertinents ? [5.3.27 à 5.3.33 ; Appendice 4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question appelant une réponse	Réponse	État de mise en œuvre
1.2-8	Y a-t-il des groupes d'action pour la sécurité qui travaillent de concert avec le comité de la sécurité (en particulier pour les organisations grandes/complexes) ? [5.3.27 à 5.3.33 ; Appendice 4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 1.3 — Nomination du personnel clé de sécurité			
1.3-1	L'organisation a-t-elle nommé une personne qualifiée pour gérer et superviser le fonctionnement quotidien du SGS ? [5.3.27 à 5.3.33 ; 5.5.2 ; Appendice 2]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.3-2	La personne qualifiée a-t-elle un accès direct ou rend-elle directement compte au Dirigeant responsable en ce qui concerne la mise en œuvre et le fonctionnement du SGS ? [5.3.27 à 5.3.33 ; 5.5.2 ; Appendice 2, 6.1]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.3-3	Le gestionnaire responsable de l'administration du SGS a-t-il d'autres responsabilités qui pourraient entrer en conflit avec son rôle de gestionnaire du SGS ou compromettre ce rôle ? [Appendice 2, 6.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.3-4	Le poste de gestionnaire du SGS est-il un poste de haute direction dont le rang n'est pas inférieur ou second par rapport à d'autres postes opérationnels ou de production ? [Appendice 2, 6.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 1.4 — Coordination de la planification des interventions en cas d'urgence			
1.4-1	[L'organisation] a-t-elle un plan d'intervention/urgence/plan d'intervention d'urgence approprié à sa taille, sa nature et sa complexité ? [Appendice 3]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.4-2	Le Plan d'intervention d'urgence/en situation d'urgence traite-t-il de tous les scénarios d'urgence/de crise possibles ou probables concernant la fourniture des produits ou services d'aviation de l'organisation ? [Appendice 3, 4 f)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.4-3	L'ERP inclut-il des procédures pour que se poursuivent en toute sécurité, la production, la fourniture ou le soutien de ses produits ou services d'aviation pendant de telles urgences ? [Appendice 3, 4 e)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.4-4	Y a-t-il un plan et des dossiers pour les exercices ou manœuvres dans le cadre de l'ERP ? [Appendice 3, 5 c)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.4-5	L'ERP traite-t-il de la coordination nécessaire de ses procédures d'intervention d'urgence avec celles d'autres organisations, le cas échéant ? [Appendice 3, 4 d)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question appelant une réponse	Réponse	État de mise en œuvre
1.4-6	[L'organisation] a-t-elle en place un processus de distribution et de communication de l'ERP à tout le personnel pertinent, y compris les organisations externes pertinentes ? [Appendice 3, 5 d)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.4-7	Y a-t-il une procédure d'examen périodique de l'ERP pour veiller à ce qu'ils restent pertinents et efficaces ? [Appendice 3, 5 f)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 1.5 — Documentation relative au SGS			
1.5-1	Y a-t-il un document récapitulatif ou document de présentation du SGS, de haut niveau, qui est approuvé par le Dirigeant responsable et accepté par l'AAC ? [5.3.36 à 5.3.38]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.5-2	La documentation relative au SGS traite-t-elle du SGS de l'organisation et de ses composants et éléments associés ? [5.3.36 à 5.3.38 ; 5.4.1 ; Appendice 4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.5-3	Le cadre du SGS de [l'organisation] est-il aligné sur le cadre du SGS réglementaire ? [5.3.36 à 5.3.38 ; 5.4.1 ; Appendice 4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.5-4	[L'organisation] tient-elle un registre des documents justificatifs pertinents concernant la mise en œuvre et le fonctionnement du SGS ? [5.3.36 à 5.3.38 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.5-5	[L'organisation] a-t-elle un plan de mise en œuvre du SGS pour établir son processus de mise en œuvre du SGS, et notamment des tâches spécifiques et des jalons de mise en œuvre correspondants ? [5.4.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.5-6	Le plan de mise en œuvre du SGS traite-t-il de la coordination entre le SGS du prestataire de services et le SGS des organisations externes, le cas échéant ? [5.4.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
1.5-7	Le plan de mise en œuvre du SGS est-il entériné par le Dirigeant responsable ? [5.4.4 ; 5.5.2]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Composant 2 — GESTION DES RISQUES DE SÉCURITÉ			
Élément 2.1 — Identification des dangers			
2.1-1	Y a-t-il un processus de comptes rendus volontaires des dangers/menaces par tous les employés ? [5.3.42 à 5.3.52 ; 5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question appelant une réponse	Réponse	État de mise en œuvre
2.1-2	Le compte rendu volontaire de dangers/menaces est-il simple, ouvert à tout le personnel qui participe aux fonctions liées à la sécurité et est-il proportionnel à la taille du prestataire de services ? [5.3.42 à 5.3.52]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.1-3	Le SDCPS de [l'organisation] comprend-il des procédures pour le compte rendu d'incidents/accidents par le personnel opérationnel ou de production ? [5.3.42 à 5.3.52 ; 5.5.4 ; Chapitre 4, Appendice 3]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.1-4	Le compte rendu d'incidents/accidents est-il simple, ouvert à tout le personnel qui participe aux fonctions liées à la sécurité et est-il proportionnel à la taille du prestataire de services ? [5.3.42 à 5.3.52 ; 5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.1-5	[L'organisation] a-t-elle des procédures pour des investigations de tous les incidents/accidents signalés ? [5.3.42 à 5.3.52 ; 5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.1-6	Y a-t-il des procédures pour veiller à ce que les dangers/menaces identifiés ou découverts lors de processus d'investigations sur des incidents/accidents soient dûment pris en compte et intégrés dans la procédure de collecte des dangers et d'atténuation des risques de l'organisation ? [2.13.9 ; 5.3.50 f) ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.1-7	Y a-t-il des procédures prévoyant d'examiner les dangers/menaces provenant de rapports pertinents de l'industrie en vue de mesures de suivi ou d'évaluation des risques, le cas échéant ? [5.3.5.1]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 2.2 — Évaluation et atténuation des risques de sécurité			
2.2-1	Y a-t-il une procédure documentée d'identification des dangers et d'atténuation des risques (HIRM) comprenant l'utilisation d'outils d'analyse objective des risques ? [2.13 ; 2.14 ; 5.3.53 à 5.3.61]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.2-2	Les comptes rendus d'évaluation des risques sont-ils approuvés par les gestionnaires de service ou à un plus haut niveau, selon le cas ? [2.15.5 ; 5.3.53 à 5.3.61]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.2-3	Y a-t-il une procédure d'examen périodique des dossiers d'atténuation des risques existants ? [5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question appelant une réponse	Réponse	État de mise en œuvre
2.2-4	Y a-t-il une procédure pour tenir compte des mesures d'atténuation chaque fois que des niveaux de risques inacceptables sont détectés ? [5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.2-5	Y a-t-il une procédure pour prioriser les dangers identifiés en vue des mesures d'atténuation des risques ? [5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
2.2-6	Y a-t-il un programme d'examen systématique et progressif de toutes les opérations, de tous les processus, installations et équipements liés à la sécurité de l'aviation qui sont soumis au processus HIRM précisé par l'organisation ? [5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Composant 3 — ASSURANCE DE LA SÉCURITÉ			
Élément 3.1 — Surveillance et mesure de la performance de sécurité			
3.1-1	Y a-t-il des indicateurs de performance de sécurité qui soient énoncés pour mesurer et surveiller la performance de sécurité des activités d'aviation de l'organisation ? [5.3.66 à 5.3.73 ; 5.4.5 ; 5.5.4 ; 5.5.5 ; Appendice 6]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-2	Les indicateurs de performance de sécurité sont-ils pertinents à la politique de sécurité de l'organisation ainsi qu'aux objectifs/buts de sécurité de haut niveau de la direction ? [5.3.66 à 5.3.73 ; 5.4.5 ; Appendice 6]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-3	Les indicateurs de performance de sécurité comprennent-ils l'établissement d'alertes et de cibles pour définir les zones de performance inacceptables et des objectifs d'amélioration planifiés ? [5.3.66 à 5.3.73 ; 5.4.5 ; 5.5.4 ; 5.5.5 ; Appendice 6]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-4	La détermination de niveaux d'alerte ou de critères de situation incontrôlable est-elle fondée sur des principes de mesures objectives de la sécurité ? [5.3.66 à 5.3.73 ; 5.4.5 ; Appendice 6]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-5	Les indicateurs de performance de sécurité comprennent-ils la surveillance quantitative de résultats de sécurité à hautes conséquences (par exemple des taux d'accidents et d'incidents graves) ainsi que d'événements à faibles conséquences (par exemple taux de non-conformité, lacunes) ? [5.3.66 à 5.3.73 ; 5.4.5 ; 5.5.4 ; 5.5.5 ; Appendice 6]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-6	Les indicateurs de performance de sécurité et leurs niveaux associés de performance sont-ils élaborés en consultation et avec l'accord de l'autorité de l'aviation civile ? [5.3.66 à 5.3.73 ; 5.4.5.2 ; 5.5.4 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question appelant une réponse	Réponse	État de mise en œuvre
3.1-7	Y a-t-il une procédure prévoyant des mesures correctrices ou de suivi lorsque des objectifs ne sont pas atteints et que les niveaux d'alerte sont dépassés/violés ? [5.4.5 ; Appendice 6, Tableau 5-A6-5 b)]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.1-8	Les indicateurs de performance de sécurité sont-ils revus périodiquement ? [5.4.5 ; Appendice 6]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 3.2 — La gestion du changement			
3.2-1	Y a-t-il une procédure d'examen des installations et équipements existants liés à la sécurité de l'aviation (y compris les dossiers HIRM) chaque fois qu'il y a des changements pertinents de ces installations ou équipements ? [5.3.74 à 5.3.77 ; 5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.2-2	Y a-t-il une procédure d'examens des opérations et processus existants liés à la sécurité de l'aviation (y compris tous les dossiers HIRM) chaque fois qu'il y a des changements pertinents de ces opérations ou processus ? [5.3.74 à 5.3.77 ; 5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.2-3	Y a-t-il une procédure d'examen des nouvelles opérations et processus liés à la sécurité de l'aviation pour en déceler les dangers/risques, avant de les mettre en service ? [5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.2-4	Y a-t-il une procédure d'examen des installations, équipements, opérations ou processus pertinents existants (y compris les dossiers HIRM) toutes les fois qu'il y a des changements pertinents externes à l'organisation, comme les normes réglementaires/de l'industrie, les meilleures pratiques ou la technologie ? [5.5.4]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 3.3 — Amélioration continue du SGS			
3.3-1	Y a-t-il une procédure d'audit/évaluation interne périodique du SGS ? [5.3.78 à 5.3.82 ; 5.5.4 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.3-2	Y a-t-il un plan actuel d'audit/évaluation du SGS interne ? [5.3.78 à 5.3.82 ; 5.5.4 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.3-3	Le plan d'audit du SGS comprend-il l'échantillonnage des évaluations de risques de sûreté achevées/existantes ? [5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

N°	Aspect à analyser ou question appelant une réponse	Réponse	État de mise en œuvre
3.3-4	Le plan d'audit du SGS comprend-il l'échantillonnage des indicateurs de performance de sécurité pour vérifier si les données sont à jour et vérifier la performance des cibles/alertes ? [5.4.5 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.3-5	Le plan d'audit du SGS couvre-t-il l'interface du SGS avec les sous-traitants ou clients, le cas échéant ? [5.4.1 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
3.3-6	Y a-t-il un processus prévoyant que les rapports d'audit/évaluation du SGS soient soumis ou transmis avec insistance au responsable, le cas échéant ? [5.3.80 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Composant 4 — PROMOTION DE LA SÉCURITÉ			
Élément 4.1 — Formation et éducation			
4.1-1	Y a-t-il un programme de formation et de familiarisation au SGS pour le personnel participant à la mise en œuvre ou au fonctionnement du SGS ? [5.3.86 à 5.3.91 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.1-2	Le Dirigeant responsable a-t-il bénéficié d'une familiarisation, d'une séance d'information ou d'une séance de formation appropriée au SGS ? [5.3.86 à 5.3.91 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.1-3	Le personnel participant à l'atténuation des risques reçoit-il une formation ou familiarisation appropriée à la gestion des risques ? [5.3.86 à 5.3.91 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.1-4	Y a-t-il des preuves d'efforts d'information ou de sensibilisation au SGS à l'échelle de l'organisation ? [5.3.86 à 5.3.91 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
Élément 4.2 — La communication relative à la sécurité			
4.2-1	[L'organisation] participe-t-elle à un partage de l'information de sécurité avec les prestataires de produits et de services ou organisations externes pertinents, notamment les organismes de réglementation de l'aviation pertinents ? [5.3.92 ; 5.3.93 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.2-2	Y a-t-il des preuves d'une publication, d'une circulaire sur la sécurité (SGS) ou de moyens de communication des questions de sécurité (SGS) aux employés ? [5.3.92 ; 5.3.93 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	
4.2-3	Le manuel et les éléments indicatifs connexes concernant le SGS de [l'organisation] sont-ils accessibles ou diffusés à tout le personnel pertinent ? [5.3.92 ; 5.3.93 ; 5.5.5]	<input type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> En partie	

2. ANALYSE DÉTAILLÉE DES ÉCARTS DU SGS ET TÂCHES DE MISE EN ŒUVRE (TABLEAU 5-A7-2)

La liste de vérification initiale de l'analyse des écarts figurant au Tableau 5-A7-1 devrait alors être suivie en utilisant le « plan d'analyse des écarts du SGS et d'identification des tâches de mise en œuvre » figurant au Tableau 5-A7-2. Une fois achevé, le Tableau 5-A7-2 permettra le suivi de l'analyse des détails des écarts et aidera à transformer ces lacunes en tâches et sous-tâches réelles requises dans le contexte spécifique des processus et procédures de l'organisation. Chaque tâche sera alors affectée en conséquence aux personnes ou groupes appropriés pour suite à donner. Il est important d'assurer dans le Tableau 5-A7-2 la corrélation entre l'élaboration des éléments/tâches individuels et la place réservée à leur description dans le document SGS afin de déclencher une mise à jour progressive du projet de document SGS à mesure que chaque élément est mis en œuvre ou renforcé. (Les textes descriptifs initiaux des éléments dans les documents SGS tendent à être anticipatoires plutôt que déclaratoires.)

3. CALENDRIER DES MESURES/TÂCHES DE MISE EN ŒUVRE (TABLEAU 5-A7-3)

Le Tableau 5-A7-3 indiquera les jalons (dates de début et de fin) prévus pour chaque tâche/action. Pour une approche de mise en œuvre par phases, ces tâches/actions devront être triées selon la phase attribuée à leurs éléments connexes. Voir la Section 5.5 du présent chapitre pour la priorisation par phase des éléments SGS, s'il y a lieu. Le Tableau 5-A7-3 peut être une récapitulation séparée de toutes les actions/tâches en souffrance ou, si l'on préfère, une continuation du Tableau 5-A7-2 sous forme d'un tableur. Lorsque l'on prévoit que le nombre réel de tâches/actions et leurs jalons sont suffisamment volumineux et complexes, de façon à nécessiter l'utilisation d'un logiciel de gestion de projet pour la mise en œuvre, cela peut être fait en utilisant des logiciels comme MS project et le diagramme de Gantt, selon le cas. Le Tableau 5-A7-4 est une illustration du diagramme de Gantt.

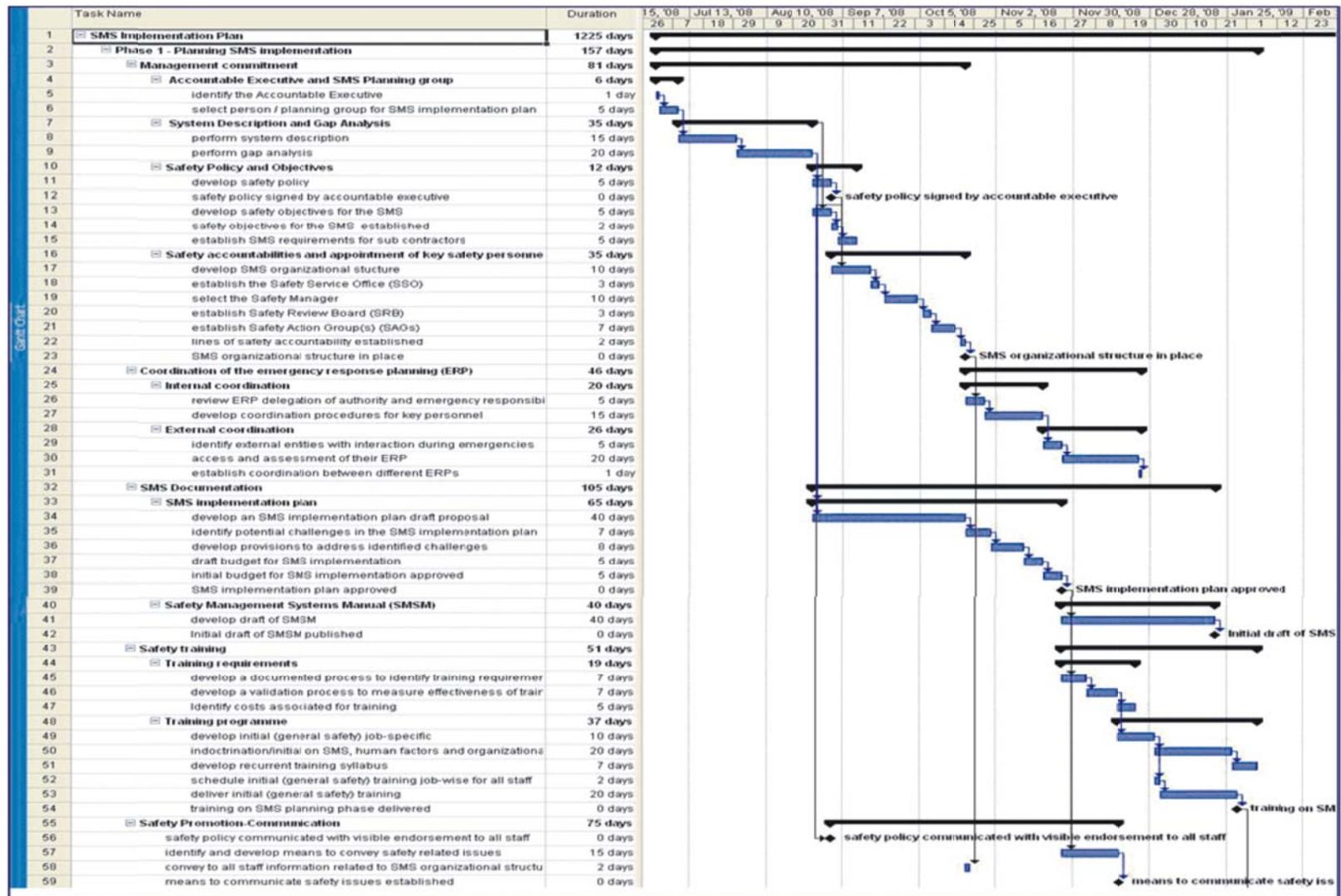
Tableau 5-A7-2. Exemple de plan SGS d'analyse des écarts et d'identification des tâches de mise en œuvre

<i>Réf. GAQ</i>	<i>Question d'analyse des écarts (GAQ)</i>	<i>Réponse (Oui/Non/ En partie)</i>	<i>Description de l'écart</i>	<i>Mesure/tâche nécessaire pour combler l'écart</i>	<i>Groupe/personne auquel est assignée la tâche</i>	<i>Référence du document SGS</i>	<i>État de la mesure/tâche (Ouverte/en cours/Fermée)</i>
1.1-1	Y a-t-il une politique de sécurité en vigueur ?	En partie	La politique de sécurité existante ne vise que l'OSHE.	<ul style="list-style-type: none"> a) renforcer la politique de sécurité en vigueur afin d'inclure les objectifs et politiques du SGS aviation ou élaborer une politique de sécurité distincte pour l'aviation ; b) faire approuver et signer la politique de sécurité par le Dirigeant responsable. 	Équipe spéciale 1	Chapitre 1, Section 1.3.	Ouverte
etc.							

Tableau 5-A7-3. Exemple de calendrier de mise en œuvre du SGS

Mesure/tâche nécessaire pour combler l'écart	Référence du document SGS	Groupe/ personne auquel est assignée la tâche	État de la mesure/ tâche	Calendrier/délai												
				1T 10	2T 10	3T 10	4T 10	1T 11	2T 11	3T 11	4T 11	1T 12	2T 12	3T 12	4T 12	etc.
1.1-1 a) Renforcer la politique de sécurité en vigueur afin d'inclure les objectifs et politiques du SGS aviation ou élaborer une politique de sécurité distincte pour l'aviation.	Chapitre 1, Section 1.3.	Équipe spéciale 1	Ouvert													
1.1-1 b) Demander que la politique de sécurité soit approuvée et signée par le Dirigeant responsable.																
etc.																

Tableau 5-A7-4. Modèle de calendrier de mise en œuvre du SGS (diagramme de Gantt)



Supplément

ÉLÉMENTS D'ORIENTATION CONNEXES DE L'OACI

MANUELS

Manuel sur les systèmes perfectionnés de guidage et de contrôle des mouvements à la surface (A-SMGCS) (Doc 9830)

Manuel des services d'aéroport (Doc 9137)

1^{re} Partie — *Sauvetage et lutte contre l'incendie*

5^e Partie — *Enlèvement des aéronefs accidentellement immobilisés*

7^e Partie — *Planification des mesures d'urgence aux aéroports*

Manuel de navigabilité (Doc 9760)

Plan mondial de navigation aérienne (Doc 9750)

Concept opérationnel d'ATM mondiale (Doc 9854)

Lignes directrices sur les facteurs humains et les systèmes de gestion du trafic aérien (Doc 9758)

Manuel de lignes directrices sur les facteurs humains en maintenance d'aéronefs (Doc 9824)

Éléments d'orientation sur les facteurs humains dans les audits de sécurité (Doc 9806)

Manuel d'instruction sur les facteurs humains (Doc 9683)

Audit de sécurité en service de ligne (LOSA) (Doc 9803)

Manuel concernant l'interception des aéronefs civils (Doc 9433)

Manuel concernant les mesures de sécurité relatives aux activités militaires pouvant présenter un danger pour les vols des aéronefs civils (Doc 9554)

Manuel d'investigations techniques sur les accidents et incidents d'aviation (Doc 9756)

Partie I — *Organisation et planification*

Partie II — *Procédures et listes de vérification*

Partie III — *Investigation*

Partie IV — *Communication des résultats*

Manuel sur les activités de dégivrage et d'antigivrage au sol des aéronefs (Doc 9640)

Manuel d'exploitation tous temps (Doc 9365)

Manuel de médecine aéronautique civile (Doc 8984)

Manuel des procédures d'inspection, d'autorisation et de surveillance continue de l'exploitation (Doc 8335)

Manuel de radiotéléphonie (Doc 9432)

Manuel sur les systèmes de guidage et de contrôle de la circulation de surface (SMGCS) (Doc 9476)

Manuel des spécifications du système de gestion du trafic aérien (Doc 9882)

Manuel sur la méthode de planification de l'espace aérien pour la détermination des minimums de séparation (Doc 9689)

Manuel sur la certification des aérodromes (Doc 9774)

Manuel sur les performances mondiales du système de navigation aérienne (Doc 9883)

Manuel sur la mise en œuvre d'un minimum de séparation verticale de 300 m (1 000 ft) entre les niveaux de vol 290 et 410 inclus (Doc 9574)

Manuel sur les organismes régionaux d'enquête sur les accidents et incidents (Doc 9946)

Manuel des performances de communication requises (RCP) (Doc 9869)

Manuel sur les opérations simultanées sur pistes aux instruments parallèles ou quasi parallèles (SOIR) (Doc 9643)

Manuel sur la prévention des incursions sur piste (Doc 9870)

Manuel sur le système de gestion de la qualité dans le domaine de l'assistance météorologique à la navigation aérienne internationale (Doc 9873)

Enquêtes de sécurité sur les opérations normales (NOSS) (Doc 9910)

Manuel de la navigation fondée sur les performances (PBN) (Doc 9613)

Manuel de supervision de la sécurité (Doc 9734)

Manuel de surveillance continue du Programme universel d'audits de supervision de la sécurité (Doc 9735)

CIRCULAIRES

Cadre unifié de modélisation des risques de collision — Document d'accompagnement du Manuel sur la méthode de planification de l'espace aérien pour l'établissement de minimums de séparation (Doc 9689) (Cir 319)

Évaluation de l'ADS-B et de la surveillance par multilatération pour l'appui aux services de la circulation aérienne et lignes directrices pour la mise en œuvre (Cir 326)

Éléments d'orientation sur l'assistance aux victimes d'accidents d'aviation et à leurs familles (Cir 285)

Dangers des lieux d'accidents d'aviation (Cir 315)

Facteurs humains. Étude n° 15 — Les facteurs humains dans la sécurité de la cabine (Cir 300)

Facteurs humains. Étude n° 16 — Facteurs transculturels dans la sécurité de l'aviation (Cir 302)

Facteurs humains. Étude n° 17 — Gestion des menaces et des erreurs (TEM) dans le contrôle de la circulation aérienne (Cir 314)

Exploitation des nouveaux avions très gros porteurs aux aérodromes existants (Cir 305)

Directives pour la formation des enquêteurs sur les accidents d'aviation (Cir 298)

— FIN —

ISBN 978-92-9249-330-1



9 7 8 9 2 9 2 4 9 3 3 0 1