OACI

Doc 9859

Manuel de gestion de la sécurité

Quatrième édition, 2018

Approuvé par la Secrétaire générale et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

OACI

Doc 9859

Manuel de gestion de la sécurité

Quatrième édition, 2018

Approuvé par la Secrétaire générale et publié sous son autorité

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, boul. Robert-Bourassa, 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
Quatrième édition, 2018

Doc 9859 — *Manuel de gestion de la sécurité*

Commande n° : 9859
ISBN 978-92-9258-699-7

AVANT-PROPOS

La présente quatrième édition du *Manuel de gestion de la sécurité* (MGS) remplace dans son intégralité la troisième édition, publiée en mai 2013. L'élaboration de la quatrième édition a été lancée après l'adoption de l'Amendement n° 1 de l'Annexe 19, afin qu'il soit tenu compte des changements introduits par cet amendement et des connaissances et de l'expérience acquises depuis la dernière révision.

Pour répondre aux besoins des différents acteurs de la communauté aéronautique qui mettent en œuvre la gestion de la sécurité et pour donner suite à une recommandation formulée par la deuxième Conférence de haut niveau sur la sécurité, qui s'est tenue en 2015, le site web consacré à la mise en œuvre de la gestion de la sécurité (www.icao.int/SMI) a été créé afin de compléter le MGS ; ce site sert de forum pour le partage des meilleures pratiques. Des exemples concrets, des outils et du matériel pédagogique d'appui seront collectés, analysés et présentés sur ce site web sur une base continue.

La présente édition est destinée à aider les États à mettre en œuvre des programmes nationaux de sécurité (PNS) efficaces. Ces programmes devront notamment veiller à ce que les prestataires de services mettent en œuvre des systèmes de gestion de la sécurité (SGS) conformément aux dispositions de l'Annexe 19. Afin d'assurer la cohérence avec les principes de gestion de la sécurité, un effort concerté a été consenti pour focaliser le propos sur le résultat attendu de chacune des normes et pratiques recommandées (SARP), en évitant à dessein de produire un texte trop normatif. L'accent a été mis sur l'importance, pour chaque organisation, d'adapter la mise en œuvre de la gestion de la sécurité à son environnement spécifique.

Note 1.— Dans le présent manuel, le terme « organisation » désigne à la fois les États et les prestataires de services.

Note 2.— Dans le présent manuel, le terme « prestataire de services » est utilisé pour désigner toute organisation du secteur aéronautique qui met en œuvre un SGS sur une base obligatoire ou volontaire, contrairement à l'Annexe 19, qui utilise ce terme pour désigner une liste très spécifique d'organisations énumérées au Chapitre 3, liste qui exclut les exploitants de l'aviation générale internationale.

La quatrième édition est subdivisée en neuf chapitres qui permettent au lecteur de développer progressivement sa compréhension de la gestion de la sécurité. Ces chapitres peuvent être regroupés sous trois thèmes, comme suit :

1) *Notions fondamentales de gestion de la sécurité* — Les Chapitres 1 à 3 développent la compréhension qu'a le lecteur des principes fondamentaux sous-tendant la gestion de la sécurité.

2) *Développement du renseignement en matière de sécurité* — Les Chapitres 4 à 7 s'appuient sur les notions fondamentales, qu'ils développent. Ces chapitres comprennent quatre sujets corrélés concernant l'exploitation des données de sécurité et des informations de sécurité pour acquérir une compréhension exploitable pouvant être utilisée par la direction d'une organisation afin de prendre des décisions fondées sur des données, y compris des décisions relatives à l'utilisation la plus efficace et la plus efficiente des ressources.

3) *Mise en œuvre de la gestion de la sécurité* — Les Chapitres 8 et 9 expliquent comment appliquer les concepts des chapitres précédents pour institutionnaliser la gestion de la sécurité au niveau de l'État et des prestataires de services.

Les orientations à l'appui des SARP relatives à la gestion de la sécurité et spécifiques au secteur qui ne figurent pas dans l'Annexe 19 (p. ex. programmes d'analyse des données de vol) ne sont pas abordées dans le présent manuel. Le *Manuel d'enquêtes sur les accidents et incidents d'aviation* (Doc 9756) donne des orientations sur la conduite d'enquêtes indépendantes sur les accidents et les incidents par les États, conformément aux dispositions de l'Annexe 13 — *Enquêtes sur les accidents et incidents d'aviation*.

L'OACI tient à souligner avec gratitude les contributions du Groupe d'experts en gestion de la sécurité (SMP) et du Groupe de la mise en œuvre de la protection des informations de sécurité (SIP IG) ainsi que des différents autres groupes d'experts et experts qui ont fourni un appui, donné des conseils et formulé des suggestions pour l'élaboration du présent manuel. Le contenu du manuel a été élaboré sur une période de deux ans et a ensuite été soumis à un examen exhaustif par des pairs, pour recueillir et prendre en compte les observations de la communauté des experts, eu égard au fait que le manuel est destiné à donner à une vaste communauté des orientations générales pour la gestion de la sécurité.

Tous les États et toutes les missions d'audit de supervision de la sécurité et missions de coopération technique de l'OACI sont invités à communiquer leurs observations concernant le présent manuel, notamment sur son application et son utilité. Il en sera tenu compte lors de l'élaboration des éditions suivantes. Les observations devraient être envoyées à l'adresse ci-après :

Secrétaire générale
Organisation de l'aviation civile internationale
999, boul. Robert-Bourassa
Montréal (Québec) H3C 5H7
Canada

TABLE DES MATIÈRES

Page

GLOSSAIRE

DÉFINITIONS

Lorsque les termes suivants sont utilisés dans ce manuel, ils ont la signification donnée ci-après :

Note.— La présence d'un astérisque à côté d'un terme indique que ce terme a déjà été défini en tant que tel dans les Annexes et les Procédures pour les services de navigation aérienne (PANS).

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

****Cible de performance de sécurité.*** Cible planifiée ou visée par l'État ou par un prestataire de services pour un indicateur de performance, qui doit être atteinte sur une période donnée et qui cadre avec les objectifs de sécurité.

****Danger.*** Situation ou objet pouvant causer un incident ou un accident d'aviation ou y contribuer.

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. Personne identifiable à qui incombe la responsabilité de la performance efficace et efficiente du SGS du prestataire de services.

****Données de sécurité.*** Ensemble défini de faits ou ensemble de valeurs de sécurité collectés de diverses sources liées à l'aviation qui est utilisé pour maintenir ou améliorer la sécurité.

Note.— Les données de sécurité proviennent d'activités proactives ou réactives concernant la sécurité, notamment les suivantes :

a) enquêtes sur des accidents ou des incidents ;

b) comptes rendus de sécurité ;

c) comptes rendus de maintien de la navigabilité ;

d) suivi des performances opérationnelles ;

e) inspections, audits, enquêtes ;

f) études et analyses de sécurité.

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.

Facteur déclencheur. Valeur établie d'un niveau ou d'un critère pour un indicateur spécifique de performance de sécurité qui sert à déclencher une action requise (p. ex. une évaluation, un ajustement ou une action correctrice).

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

***Indicateur de performance de sécurité.** Paramètre basé sur des données utilisé pour le suivi et l'évaluation de la performance de sécurité.

***Informations de sécurité.** Données de sécurité traitées, organisées ou analysées dans un contexte donné de manière à être utiles pour la gestion de la sécurité.

***Niveau acceptable de performance de sécurité (ALoSP).** Niveau de performance en matière de sécurité convenu par les autorités d'un État pour le système de l'aviation civile de cet État, comme défini dans le programme national de sécurité (PNS), exprimé en termes de cibles de performance de sécurité et d'indicateurs de performance de sécurité.

***Objectif de sécurité.** Brève déclaration de haut niveau sur les réalisations en matière de sécurité ou sur le résultat escompté à atteindre par le programme national de sécurité ou par le système de gestion de la sécurité du prestataire de services.

Note.— Les objectifs de sécurité sont définis à partir des principaux risques de sécurité d'une organisation et devraient être pris en compte durant l'établissement ultérieur de cibles et d'indicateurs de performance de sécurité.

***Performance de sécurité.** Résultats d'un État ou d'un prestataire de services en matière de sécurité, par rapport aux cibles et aux indicateurs de performance de sécurité qu'il s'est fixés.

***Programme national de sécurité (PNS).** Ensemble intégré de règlements et d'activités qui visent à améliorer la sécurité.

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

***Sécurité.** État dans lequel les risques liés aux activités aéronautiques concernant, ou appuyant directement, l'exploitation des aéronefs sont réduits et maîtrisés à un niveau acceptable.

***Supervision de la sécurité.** Fonction exécutée par un État pour s'assurer que les personnes et les organisations qui exercent une activité aéronautique respectent les lois et les règlements nationaux concernant la sécurité.

***Surveillance.** Activités par lesquelles un État vérifie de façon proactive, au moyen d'inspections et d'audits, que les titulaires de licences, de certificats, d'autorisations ou d'approbations aéronautiques se conforment en permanence aux exigences établies et fonctionnent au niveau de compétence et de sécurité requis par l'État.

***Système.** Structure organisée, intentionnelle, constituée d'éléments et composants corrélés et interdépendants et de politiques, procédures et pratiques connexes créées pour effectuer une activité spécifique ou pour résoudre un problème.

***Système de gestion de la sécurité (SGS).** Approche systématique de la gestion de la sécurité, comprenant les structures organisationnelles, l'obligation de rendre compte, les responsabilités, les politiques et les procédures nécessaires.

ABRÉVIATIONS ET SIGLES

AAC	Autorité de l'aviation civile
ADREP	Compte rendu d'accident/incident
AIA	Service d'enquête sur les accidents
ALoSP	Niveau acceptable de performance de sécurité
AOC	Permis d'exploitation aérienne
ATS	Services de la circulation aérienne
CVR	Enregistreur de conversations de poste de pilotage
Doc	Document
ERP	Plan d'intervention en cas d'urgence
FDA	Analyse des données de vol
FDR	Enregistreur de données de vol
FRMS	Système de gestion des risques de fatigue
GASP	Plan pour la sécurité de l'aviation dans le monde
GRS	Gestion des risques de sécurité
iSTARS	Système intégré d'analyse et de compte rendu des tendances de la sécurité
LOSA	Audit de sécurité en service de ligne
MGS	Manuel de gestion de la sécurité
OACI	Organisation de l'aviation civile internationale
OSHE	Sécurité, santé et environnement professionnels
PDFD	Processus décisionnel fondé sur les données
PIRG	Groupe régional de planification et de mise en œuvre
PNS	Programme national de sécurité
RASG	Groupe régional de sécurité de l'aviation
RSOO	Organisation régionale de supervision de la sécurité
SAG	Groupe d'action pour la sécurité
SARP	Normes et pratiques recommandées
SD	Écart type
SDCPS	Système de collecte et de traitement des données de sécurité
SGF	Système de gestion financière
SGQ	Système de gestion de la qualité
SGS	Système de gestion de la sécurité
SGSST	Système de gestion de la santé et de la sécurité au travail
SGSûr	Système de gestion de la sûreté
SMP	Groupe d'experts en gestion de la sécurité
SPI	Indicateur de performance de sécurité
SPT	Cible de performance de sécurité
SRB	Commission d'examen de la sécurité
SRBS	Surveillance fondée sur le risque pour la sécurité
SSO	Supervision de la sécurité par l'État
STDEVP	Écart type de la population
TNA	Analyse des besoins de formation
USOAP	Programme universel d'audits de supervision de la sécurité

PUBLICATIONS

(mentionnées dans le présent manuel)

Les documents ci-après sont cités en référence dans le présent manuel et/ou donnent des indications supplémentaires.

DOCUMENTS DE L'OACI

Annexes à la Convention relative à l'aviation civile internationale

Annexe 1 — *Licences du personnel*

Annexe 6 — *Exploitation technique des aéronefs*
Partie 1 — *Aviation de transport commercial international — Avions*
Partie 2 — *Aviation générale internationale — Avions*

Annexe 8 — *Navigabilité des aéronefs*

Annexe 13 — *Enquêtes sur les accidents et incidents d'aviation*

Annexe 14 — *Aérodromes*
Volume I — *Conception et exploitation technique des aérodromes*

Annexe 18 — *Sécurité du transport aérien des marchandises dangereuses*

Annexe 19 — *Gestion de la sécurité*

PANS

Procédures pour les services de navigation aérienne (PANS) — Aérodromes (Doc 9981)

Procédures pour les services de navigation aérienne — Gestion du trafic aérien (PANS-ATM, Doc 4444)

Manuels

Manuel des services d'aéroport (Doc 9137), Partie 3 — *Prévention et atténuation du risque faunique*

Manuel de planification des services de la circulation aérienne (Doc 9426)

Manuel de navigabilité (Doc 9760)

Manuel de sûreté de l'aviation (Doc 8973 — Diffusion restreinte)

Plan pour la sécurité de l'aviation dans le monde (GASP) (Doc 10004)

Manuel d'enquêtes sur les accidents et incidents d'aviation (Doc 9756)
Partie I — *Organisation et planification*
Partie II — *Procédures et listes de vérification*
Partie III — *Enquêtes*
Partie IV — *Communication des résultats*

Manuel pour la supervision des approches de gestion de la fatigue (Doc 9966)

Manuel sur les émetteurs laser et la sécurité des vols (Doc 9815)

Manuel sur les systèmes d'aéronef télépiloté (RPAS) (Doc 10019)

Manuel sur les compétences des inspecteurs de la sécurité de l'aviation civile (Doc 10070)

Manuel du système OACI d'information sur les impacts d'oiseaux (IBIS) (Doc 9332)

Manuel relatif à la protection des informations sur la sécurité (Doc 10053)
Partie I — *Protection des éléments d'enquête sur les accidents et les incidents*

Manuel de supervision de la sécurité (Doc 9734)
Partie A — *Mise en place et gestion d'un système national de supervision de la sécurité*
Partie B — *Mise en place et gestion d'une organisation régionale de supervision de la sécurité*

Instructions techniques pour la sécurité du transport aérien des marchandises dangereuses (Doc 9284)

———————

Chapitre 1

INTRODUCTION

1.1 QU'ENTEND-ON PAR GESTION DE LA SÉCURITÉ ?

1.1.1 La gestion de la sécurité vise à atténuer de manière proactive les risques de sécurité avant que ceux-ci n'entraînent des accidents et des incidents d'aviation. La mise en œuvre de la gestion de la sécurité permet aux États de gérer leurs activités de sécurité d'une façon plus disciplinée, intégrée et ciblée. En ayant une compréhension claire de leur rôle et de leur contribution à une exploitation sûre, les États, et leurs industries aéronautiques, peuvent donner la priorité à des actions visant à réduire les risques de sécurité et peuvent gérer leurs ressources plus efficacement afin d'optimaliser la sécurité aérienne.

1.1.2 Les activités de gestion de la sécurité d'un État voient leur efficacité renforcée lorsqu'elles sont mises en œuvre d'une façon formelle et institutionnalisée, par le biais d'un programme national de sécurité (PNS) et de systèmes de gestion de la sécurité (SGS) chez les prestataires de services. Un programme national de sécurité, combiné aux SGS des prestataires de services, pare systématiquement aux risques de sécurité, améliore la performance de sécurité de chaque prestataire de services, et, collectivement, améliore la performance de sécurité de l'État.

1.1.3 Chaque État élabore et tient à jour un PNS en tant qu'approche structurée visant à soutenir la gestion de la performance de sécurité de son aviation. La cote de sécurité actuelle de l'aviation est atteinte par le biais d'une approche traditionnelle basée sur la conformité et devrait être utilisée comme base du PNS. Les États devraient s'assurer qu'ils ont mis en place des systèmes efficaces de supervision de la sécurité. De plus amples informations sur le PNS figurent au Chapitre 8.

1.1.4 L'État doit exiger qu'un SGS soit élaboré et tenu à jour par les prestataires de services qui relèvent de son autorité, tels qu'ils sont identifiés à l'Annexe 19 — *Gestion de la sécurité*, afin d'améliorer en permanence la performance de sécurité par l'identification des dangers, la collecte et l'analyse des données et l'évaluation et la gestion en continu des risques de sécurité (voir § 1.2 pour plus de détails sur l'application du SGS). De plus amples informations sur la mise en œuvre d'un SGS figurent au Chapitre 9.

1.1.5 Dans ses objectifs, le *Plan pour la sécurité de l'aviation dans le monde (GASP)* de l'OACI (Doc 10004) appelle les États à mettre en place des systèmes solides et durables de supervision de la sécurité et à les faire évoluer progressivement vers des moyens plus élaborés de gestion de la performance de sécurité. Ces objectifs s'inscrivent dans la droite ligne des exigences de l'OACI pour la mise en œuvre de PNS par les États et de SGS par les prestataires de services.

1.1.6 Cette approche de la sécurité basée sur la performance produit des améliorations car elle se concentre sur la réalisation du résultat souhaité plutôt que sur la seule vérification de la conformité d'un État. Il importe toutefois de noter que la mise en œuvre d'une approche de la sécurité basée sur la performance est un projet collaboratif car elle exige des efforts, d'une part, du secteur aéronautique, pour élaborer des moyens appropriés permettant d'atteindre les résultats spécifiés et, d'autre part, des États, pour évaluer l'approche de chaque prestataire de services.

1.1.7 Avantages de la gestion de la sécurité

La mise en œuvre de la gestion de la sécurité offre de nombreux avantages, notamment :

a) *Une culture de la sécurité renforcée* — Il est possible de renforcer la culture de la sécurité d'une organisation en rendant visible l'engagement de la direction et en associant activement le personnel à la gestion des risques de sécurité. Quand la sécurité est activement soutenue par la direction en tant que priorité, elle est généralement bien perçue par le personnel et devient partie intégrante des opérations normales.

b) *Une approche documentée, fondée sur les processus, pour assurer la sécurité* — Elle établit une approche claire et documentée, compréhensible pour le personnel et facile à expliquer à d'autres, pour assurer la sécurité de l'exploitation. De plus, une définition claire de la performance de référence permet de réaliser des changements contrôlés dans le cadre de l'amélioration continue du programme/système de sécurité, ce qui aide l'organisation à optimaliser les ressources requises pour mettre en œuvre les changements.

c) *Une meilleure compréhension des interfaces et relations liées à la sécurité* — Le processus de documentation et de définition des interfaces de la gestion de la sécurité peut être bénéfique pour la compréhension qu'a l'organisation des relations entre les processus, ce qui génère une meilleure compréhension du processus de bout en bout et met en lumière les possibilités d'améliorer l'efficacité.

d) *Un renforcement de la détection précoce des dangers pour la sécurité* — Améliore la capacité des États/prestataires de services à détecter des problèmes de sécurité naissants, ce qui peut prévenir des accidents et des incidents grâce à l'identification proactive des dangers et à la gestion des risques de sécurité.

e) *Un processus décisionnel fondé sur les données de sécurité* — Améliore la capacité des États/ prestataires de services à recueillir des données de sécurité à des fins d'analyse de sécurité. Une réflexion stratégique visant à déterminer les questions auxquelles il convient de répondre permet d'obtenir des informations sur la sécurité susceptibles d'aider les décideurs à prendre des décisions valables, en meilleure connaissance de cause, quasi en temps réel. Un aspect important de ce processus décisionnel est l'affectation des ressources aux domaines où les besoins ou les inquiétudes sont les plus grands.

f) *Une amélioration de la communication en matière de sécurité* — Fournit un langage commun en matière de sécurité dans l'ensemble d'une organisation ou d'un secteur d'activité. Un langage commun en matière de sécurité est un élément crucial permettant de développer une compréhension commune des objectifs et réalisations de l'organisation en matière de sécurité. En particulier, il livre une appréciation des objectifs de sécurité de l'organisation, de ses indicateurs de performance de sécurité (SPI) et de ses cibles de performance de sécurité (SPT), qui donnent orientations et motivation en matière de sécurité. Le personnel sera plus conscient de la performance de l'organisation et des progrès engrangés vers la réalisation des objectifs de sécurité définis, ainsi que de sa contribution au succès de l'organisation. Le langage commun en matière de sécurité permet aux prestataires de services ayant de multiples entreprises aéronautiques de regrouper les informations de sécurité pour toutes les entités de l'organisation. Il est nécessaire de soutenir la gestion des interfaces dans l'ensemble du système aéronautique.

g) *Des preuves que la sécurité est une priorité* — Ces preuves montrent comment la direction soutient et favorise la sécurité, comment les risques de sécurité sont identifiés et gérés et comment la performance de sécurité est améliorée en continu, ce qui accroît la confiance de la communauté aéronautique à l'intérieur comme à l'extérieur de l'organisation. Ces preuves donnent aussi au personnel confiance dans la performance de sécurité de l'organisation, ce qui peut attirer et fidéliser

davantage de personnels hautement qualifiés. Elles permettent en outre aux États et aux organisations régionales de supervision de la sécurité (RSOO) de renforcer la confiance dans la performance de sécurité des prestataires de services.

h) *Des économies possibles* — Peuvent permettre à certains prestataires de services de répondre aux conditions d'obtention d'une réduction de leurs primes d'assurance et/ou d'une réduction des primes de leur régime d'indemnisation des travailleurs sur la base des résultats de leur SGS.

i) *Une amélioration de l'efficacité* — Éventuelle réduction du coût de l'exploitation par la mise en lumière des inefficacités dans les processus et systèmes existants. L'intégration avec d'autres systèmes de gestion internes ou externes peut aussi permettre de réaliser des économies sur des coûts supplémentaires.

j) *Un évitement des coûts* — Par l'identification proactive des dangers et par la gestion des risques de sécurité (GRS), il est possible d'éviter les coûts dus à des accidents et à des incidents. Dans ces cas, les coûts directs peuvent inclure les blessures, les dommages aux biens, les réparations d'équipements et les retards d'exécution. Les coûts indirects peuvent inclure des actions en justice, des pertes de parts de marché, une baisse de réputation, des excédents de pièces détachées, des outils et des formations, une hausse des primes d'assurance, des pertes de productivité du personnel, la remise en état et le nettoyage des équipements, la perte d'utilisation d'équipements entraînant un remplacement à court terme d'équipements, et des enquêtes internes.

1.2 CHAMP D'APPLICATION DE LA GESTION DE LA SÉCURITÉ

Les responsabilités de l'État en matière de gestion de la sécurité sont énoncées à l'Annexe 19, Chapitre 3, et incluent d'imposer la mise en œuvre d'un SGS aux prestataires de services mentionnés dans les SARP. Les dispositions relatives à la mise en œuvre de SGS par les prestataires de services figurent au Chapitre 4 et à l'Appendice 2 de l'Annexe 19.

1.2.1 Champ d'application d'un SGS

1.2.1.1 L'évaluation permettant de déterminer le champ d'application d'un SGS pour l'Amendement n° 1 à l'Annexe 19 reposait sur un ensemble de critères. Ces mêmes critères sont censés être utilisés périodiquement par l'OACI et par le Groupe d'experts en gestion de la sécurité (SMP) pour réévaluer la nécessité d'étendre le champ d'application à d'autres organisations de l'aviation.

Approche de la sécurité visant l'ensemble d'un système

1.2.1.2 Une approche de la sécurité visant l'ensemble d'un système considère l'industrie aéronautique dans son entièreté comme un système. Tous les prestataires de services et leurs systèmes de gestion de la sécurité sont considérés comme des sous-systèmes. Cela permet aux États d'étudier les interactions et les mécanismes de cause à effet dans l'ensemble du système. Il est souvent impossible ou inenvisageable de constituer tous les systèmes de sécurité de la même manière. C'est pourquoi une préoccupation essentielle pour les États et les prestataires de services est de déterminer comment gérer au mieux les interfaces entre des systèmes dissemblables en interaction.

1.2.1.3 Lors de l'examen du champ d'application des SGS, le lien entre prestataires de services déjà soumis à l'obligation d'avoir un SGS en vertu de l'Annexe 19 et d'autres organisations ayant des activités dans le secteur aéronautique a été analysé. La mise en place d'un SGS devrait réduire le risque de lacunes ou de chevauchements en matière de sécurité et non accroître les risques de sécurité du fait d'une diminution de l'interopérabilité.

Incidences de la sous-traitance

1.2.1.4 Pour que la GRS soit efficace parmi tous les prestataires de services, il importe de définir clairement les responsabilités d'identification des dangers et de gestion des risques de sécurité connexes dans l'ensemble de la chaîne de services au sein du système, sans lacunes ni chevauchements. Lorsqu'un prestataire de services soumis à l'obligation de mise en place d'un SGS sous-traite à une organisation non soumise à l'obligation d'avoir un SGS, les dangers et risques de sécurité potentiellement introduits par le sous-traitant sont abordés par le SGS du prestataire de services. Cela confère des responsabilités supplémentaires en matière de GRS au prestataire de services, qui doit s'assurer qu'il connaît les risques de sécurité induits par les activités de son ou de ses sous-traitants. Pour de plus amples informations sur la GRS, voir le Chapitre 2.

Maîtrise des risques de sécurité au moyen des réglementations

1.2.1.5 Il convient que les États évaluent si la législation et les réglementations existantes parent efficacement aux dangers induits par l'activité. Il se pourrait que les exigences existantes assurent une atténuation suffisante des risques de sécurité et qu'exiger un SGS d'organisations auxquelles l'Annexe 19 n'en impose pas n'améliore pas de façon substantielle la sécurité.

1.2.2 Extension du champ d'application discrétionnaire du SGS

1.2.2.1 Les critères d'applicabilité exposés ci-dessus peuvent aussi servir d'orientations pour les États qui envisagent d'étendre le champ d'application du SGS au-delà de celui que définit l'Annexe 19 ou de promouvoir une mise en œuvre volontaire. La mise en place d'un champ d'application discrétionnaire du SGS doit être mûrement réfléchie. La décision d'étendre le champ d'application du SGS à des secteurs ou à des prestataires de services devrait tenir compte des risques pour la sécurité identifiés dans l'État et, si la décision est prise, la mise en œuvre du SGS devrait faire l'objet d'un suivi dans le cadre du PNS. Avant d'exiger un SGS, les États sont invités à étudier :

a) s'il existe toute autre option viable pour réaliser l'amélioration souhaitée de la performance de sécurité ;

b) si des ressources suffisantes sont disponibles pour que l'État et le secteur concerné puissent mettre en œuvre le SGS et en assurer le suivi. En particulier, il convient de tenir compte d'éventuelles incidences sur la dotation en personnel et de la difficulté potentielle d'acquérir et d'intégrer les compétences et connaissances nécessaires.

1.2.2.2 Tout État devrait examiner le niveau acceptable de performance de sécurité (ALoSP) dans son industrie aéronautique et instituer le régime d'application du SGS le plus susceptible d'atteindre les objectifs de l'État en matière de sécurité. Le régime d'application du SGS adopté évoluera probablement parallèlement à l'ALoSP de l'État.

1.2.3 Responsabilités de l'État en matière de gestion de la sécurité

Aucune disposition de l'Annexe 19 ne vise à transférer à l'État les responsabilités du prestataire ou de l'exploitant de services aéronautiques. Les États possèdent de nombreux outils pour gérer la sécurité au sein de leurs systèmes. Dans le cadre de son PNS, chaque État devrait étudier les meilleures options pour la supervision d'activités aéronautiques susceptibles de ne pas relever du champ d'application des Annexes actuelles de l'OACI ou pour la supervision d'activités nouvelles ou émergentes.

1.2.4 Applicabilité aux prestataires de services militaires ou appartenant à l'État

1.2.4.1 Dans certains États, la fonction de prestataire de services est assurée par la fonction publique ou par l'armée. Certains prestataires de services civils fournissent des services contractuels à l'armée et certaines organisations militaires fournissent des services civils. Indépendamment des arrangements, le prestataire de services pour des activités civiles au sein de l'État devrait être tenu de respecter toutes les SARP de l'OACI applicables, y compris les exigences de SGS énoncées dans l'Annexe 19, sans tenir compte de la nature spécifique d'une telle organisation. La description du système de l'État ou du prestataire de services devrait tenir compte des fonctions de ces organisations et de leurs relations entre elles. Le dirigeant responsable du prestataire de services, que celui-ci soit civil ou militaire, devrait être à même d'expliquer les arrangements et la façon dont les risques de sécurité sont gérés. Pour faire simple, les prestataires de services devraient gérer la sécurité indépendamment des arrangements organisationnels.

1.2.4.2 Lorsque l'État opère comme prestataire de services, il devrait y avoir une séparation claire entre ses fonctions en tant que prestataire de services et ses fonctions d'autorité nationale de réglementation. Pour assurer cette séparation, il faut définir clairement les rôles et responsabilités du personnel de l'autorité nationale de réglementation et du personnel du prestataire de services, afin d'éviter des conflits d'intérêts.

1.2.5 Sécurité, santé et environnement professionnels ou sécurité aérienne

La sécurité, la santé et l'environnement professionnels (OSHE) (on parle aussi de santé et sécurité au travail [SST]) est un domaine qui s'intéresse à la sécurité, à la santé et au bien-être des personnes au travail. La principale différence entre les systèmes de gestion de la sécurité aérienne et d'OSHE réside dans l'intention. Dans nombre d'États, les employeurs ont un devoir légal de veiller raisonnablement à la santé et à la sécurité de leurs employés. L'intention des programmes d'OSHE est d'assumer les obligations légales et éthiques des employeurs en favorisant un environnement de travail sûr et sain. Ces problématiques sont normalement abordées par des organes gouvernementaux différents de ceux qui traitent des questions aéronautiques. L'Annexe 19, Chapitre 2, *Application*, se concentre intentionnellement sur les « fonctions de gestion de la sécurité qui concernent ou appuient directement la sécurité de l'exploitation des aéronefs ».

1.3 MISE EN ŒUVRE DE LA GESTION DE LA SÉCURITÉ

1.3.1 Il est essentiel de créer une base solide pour parvenir à une mise en œuvre efficace de la gestion de la sécurité. Les aspects suivants devraient être abordés en tant que premières étapes de la mise en œuvre des exigences relatives au PNS ou au SGS :

a) *Engagement de la haute direction :* Il est indispensable que la haute direction de tous les organismes aéronautiques de l'État s'engage à réaliser une mise en œuvre efficace de la gestion de la sécurité.

b) *Conformité aux exigences normatives :* L'État devrait veiller à ce qu'un système éprouvé de supervision de la sécurité soit en place pour l'octroi des licences, certifications, autorisations et approbations d'individus et d'organisations exerçant des activités aéronautiques sur son territoire, y compris pour le personnel technique qualifié. Les prestataires de services devraient garantir qu'ils ont mis en place des processus pour assurer une conformité constante aux exigences normatives établies.

c) *Régime d'exécution :* L'État devrait instaurer une politique d'exécution et des cadres pour permettre aux parties de gérer et résoudre les écarts et les violations mineures.

d) *Protection des informations de sécurité :* Il est essentiel que les États mettent en place un cadre juridique de protection afin de garantir la disponibilité en continu de données de sécurité et d'informations de sécurité.

1.3.2 Description du système

La description du système est un résumé des processus, activités et interfaces de l'organisation (État ou prestataire de services) qui doivent être évalués aux fins de l'identification des dangers et de l'évaluation des risques de sécurité, comme prévu dans le système de sécurité de ladite organisation. Elle décrit le système aéronautique dans lequel fonctionne l'organisation, ainsi que les diverses entités et autorités concernées. Elle inclut les interfaces au sein de l'organisation ainsi que les interfaces avec des organisations extérieures qui contribuent à une prestation sûre de services. La description du système fournit un point de départ pour la mise en œuvre du PNS/SGS. De plus amples informations sur la description du système pour les États et les prestataires de services figurent aux Chapitres 8 et 9, respectivement.

1.3.3 Interfaces

1.3.3.1 Lorsque les États et les prestataires de services envisagent de mettre en œuvre une gestion de la sécurité, il est important qu'ils prennent en considération les risques de sécurité induits par les interfaces entre les entités. Les interfaces peuvent être internes (p. ex. entre l'exploitation et la maintenance ou entre les services des finances, des ressources humaines ou le service juridique) ou elles peuvent être externes (p. ex. un autre État, des prestataires de services ou des entités auxquelles des services sont sous-traités). Lorsque les interfaces sont identifiées et gérées, les États et les prestataires de services ont une meilleure maîtrise de tout risque de sécurité connexe. Les interfaces sont définies dans le cadre de la description du système.

Évaluation des incidences des interfaces sur la sécurité

1.3.3.2 Une fois qu'un État ou un prestataire de services a identifié ses interfaces, le risque de sécurité posé par chacune des interfaces est évalué à l'aide des processus mis en place par l'organisation pour l'évaluation des risques de sécurité (voir Chapitre 2 pour plus de détails). Sur la base des risques de sécurité identifiés, l'État ou le prestataire de services peut envisager de travailler avec d'autres organisations pour établir une stratégie appropriée de maîtrise des risques de sécurité. Les organisations qui travaillent en collaboration peuvent être à même d'identifier plus de dangers aux interfaces, d'évaluer tout risque de sécurité connexe et d'établir des contrôles appropriés pour les parties concernées par ces interfaces. Une collaboration est hautement souhaitable parce que la perception des risques de sécurité peut varier d'une organisation à l'autre.

1.3.3.3 Il importe aussi de reconnaître qu'il incombe à chaque organisation concernée d'identifier et de gérer tout danger identifié qui l'affecte. La criticité de l'interface peut varier d'une organisation à l'autre. Chaque organisation pourrait raisonnablement appliquer des classifications différentes des risques de sécurité et avoir des priorités différentes en matière de risques de sécurité (pour ce qui est des performances de sécurité, des ressources, de la durée).

Suivi et gestion des interfaces

1.3.3.4 Les États et les prestataires de services sont responsables du suivi et de la gestion en continu de leurs interfaces afin de garantir une prestation sûre de services. Une approche efficace de la gestion des risques de sécurité aux interfaces est d'établir des accords formels entre les organisations en interface, avec des responsabilités de suivi et de gestion clairement définies. La documentation et le partage de tous les problèmes de sécurité aux interfaces, des comptes rendus de sécurité et des leçons tirées ainsi que des risques de sécurité entre les organisations en interface

garantiront une compréhension claire de ces problématiques. Le partage permet un transfert de connaissances et de pratiques de travail susceptible d'améliorer l'efficacité de la sécurité de chaque organisation.

1.3.4 Planification de la mise en œuvre

1.3.4.1 La réalisation d'une analyse des carences avant le lancement de la mise en œuvre du PNS/SGS permettra à l'organisation d'identifier les carences entre les structures et processus organisationnels existants et ceux qui sont requis pour un fonctionnement efficace du PNS ou du SGS. Pour le PNS, il importe d'inclure un examen des questions de protocoles du Programme universel d'audits de supervision de la sécurité (USOAP) qui sont considérées comme la base du PNS.

1.3.4.2 Le plan de mise en œuvre du PNS ou du SGS est, comme son nom l'indique, un plan pour la mise en œuvre du PNS/SGS. Il donne une description claire des ressources, tâches et processus requis et un calendrier et un ordre indicatifs pour les tâches et responsabilités principales. De plus amples informations sur la mise en œuvre de la gestion de la sécurité à l'attention des États et des prestataires de services figurent aux Chapitres 8 et 9, respectivement.

Évaluation de la maturité

1.3.4.3 Peu après la mise en œuvre des composants et éléments clés du PNS ou du SGS, des évaluations périodiques devraient être menées pour surveiller l'efficacité du système mis en place. À mesure que le système gagne en maturité, l'organisation devrait veiller à s'assurer qu'il fonctionne comme prévu et est efficace pour atteindre ses objectifs et cibles de sécurité explicites. La gestion de la sécurité prend du temps pour atteindre sa maturité et le but devrait être de maintenir ou de constamment améliorer la performance de sécurité de l'organisation.

1.3.5 Considérations relatives à la taille et à la complexité

1.3.5.1 Chaque État et chaque prestataire de services sont différents. Les PNS et les SGS sont conçus sur mesure pour répondre aux besoins spécifiques de chaque État ou prestataire de services. Tous les composants et tous les éléments des PNS/SGS sont interconnectés et interdépendants et sont nécessaires pour assurer un fonctionnement efficace. Il est important que les exigences du PNS et du SGS ne soient pas mises en œuvre uniquement de façon normative. Les exigences normatives traditionnelles doivent être complétées par une approche basée sur la performance.

1.3.5.2 Le programme/système est conçu pour que chaque organisation puisse atteindre les résultats escomptés sans fardeau excessif. Mis en œuvre correctement, le PNS et le SGS visent à compléter et renforcer les systèmes et processus existants de l'organisation. Une gestion efficace de la sécurité sera réalisée par le biais d'une planification et d'une mise en œuvre bien réfléchies, qui garantissent que chaque exigence soit abordée d'une manière adaptée à la culture et à l'environnement opérationnel de l'organisation. De plus amples informations sur les aspects à envisager lors de la mise en œuvre d'un PNS/SGS pour les États et les prestataires de services figurent aux Chapitres 8 et 9, respectivement.

1.3.6 Intégration des éléments fondamentaux

Il convient de noter que tous les systèmes sont composés de trois éléments fondamentaux : les personnes, les processus et la technologie. La gestion de la sécurité ne fait pas exception. Dans le cadre de l'établissement ou du maintien des différents processus, activités et fonctions, tous les États et prestataires de services devraient s'assurer qu'ils ont tenu compte de l'intention derrière chaque exigence et, plus important encore, de la façon dont ils vont travailler ensemble pour permettre à l'organisation d'atteindre ses objectifs de sécurité. Chacun de ces éléments de la gestion de la sécurité, et les relations entre eux, seront couverts dans ce manuel.

1.4 GESTION INTÉGRÉE DES RISQUES

1.4.1 Le système d'aviation dans son ensemble comprend de nombreux systèmes fonctionnels différents, tels que la finance, l'environnement, la sécurité et la sûreté. Ces deux derniers sont les principaux domaines opérationnels de l'ensemble du système aéronautique. En tant que concepts, ils partagent d'importantes caractéristiques car ils s'intéressent au risque d'événements pouvant entraîner des conséquences de degrés de gravité divers. Toutefois, ils diffèrent par l'élément important qu'est l'intention. La sûreté vise les actes malveillants intentionnels destinés à perturber la performance d'un système. La sécurité se concentre sur l'incidence négative que des conséquences involontaires d'un ensemble de facteurs peuvent avoir sur la performance des systèmes concernés.

1.4.2 Dans le contexte opérationnel, tous les systèmes fonctionnels induisent une certaine forme de risque qui doit être gérée de façon adéquate pour atténuer toute conséquence négative. Traditionnellement, chaque système a élaboré des cadres et pratiques spécifiques au secteur pour la gestion des risques, afin de tenir compte des spécificités de chaque système. La plupart de ces pratiques de gestion des risques comprennent une analyse complète des conséquences à l'intérieur du système, souvent appelée « gestion des conséquences involontaires ». Un autre aspect vise les conséquences intersystèmes qui résultent des processus de gestion des risques spécifiques aux systèmes. Il concerne le fait qu'une stratégie efficace de gestion des risques d'un secteur spécifique peut avoir une incidence négative sur un autre secteur opérationnel de l'aviation. Dans le domaine aéronautique, la dépendance entre systèmes la plus soulignée est le dilemme entre sécurité et sûreté. Des mesures de sûreté efficaces peuvent avoir des incidences négatives sur la sécurité, et inversement. Les domaines de la sécurité et de la sûreté peuvent différer par l'élément de l'intention sous-jacente mais ils convergent dans leur but commun de protéger les personnes et les biens (p. ex. la gestion des cyberattaques et des risques requiert une coordination dans l'ensemble des domaines de la sécurité et de la sûreté de l'aviation). Dans certains cas, la gestion du risque inhérent de l'un peut affecter l'autre domaine de façons imprévues, comme le révèlent les exemples suivants :

a) les portes de poste de pilotage renforcées rendues nécessaires en raison des risques de sûreté peuvent avoir des implications sur la sécurité de l'exploitation d'un aéronef ;

b) les restrictions imposées au transport d'appareils électroniques personnels dans la cabine peuvent déplacer le risque de sûreté de la cabine à la soute, ce qui accroît le risque de sécurité ;

c) un changement de routes pour éviter le survol de zones de conflit peut encombrer des couloirs aériens et ainsi générer un problème de sécurité.

1.4.3 Une gestion réussie des risques en aviation devrait viser une réduction générale des risques au sein du système, y compris au sein de tous les systèmes fonctionnels concernés. Ce processus exige l'évaluation analytique de l'ensemble du système au plus haut niveau de l'entité concernée (État, organisations régionales, prestataires de services). L'évaluation et l'intégration des besoins et de l'interdépendance des systèmes fonctionnels constituent ce qu'il est convenu d'appeler la gestion intégrée des risques (GIR). La GIR vise une réduction globale des risques de l'organisation. À cette fin, elle s'appuie sur une analyse quantitative et qualitative à la fois des risques inhérents et de l'efficacité et de l'incidence des processus de gestion des risques spécifiques au secteur. La GIR assume, à l'échelle du système, une responsabilité de coordonner, harmoniser et optimiser les processus de gestion des risques avec pour unique but la réduction des risques. La GIR ne peut remplacer les gestions des risques spécifiques en place pour les systèmes fonctionnels et n'entend pas déléguer à ces gestions des tâches et responsabilités supplémentaires. La GIR est un concept de haut niveau distinct, destiné à exploiter les conseils éclairés des responsables de la gestion des risques spécifiques au secteur et à fournir des rétro-informations complètes afin d'atteindre le plus haut niveau de performance des systèmes à un niveau socialement acceptable. Les Chapitres 2, 8 (pour les États) et 9 (pour les prestataires de services) donnent plus d'informations sur la gestion des risques pour la sécurité, dans les limites du présent manuel.

Note.— La structure et les domaines de responsabilité du gouvernement au sein de l'État peuvent affecter la supervision de chaque domaine. Par exemple, l'autorité de l'aviation civile (AAC) peut être chargée de la sécurité de l'aviation tandis que l'agence de protection de l'environnement peut être compétente pour la supervision de l'environnement. Chaque entité chargée de la supervision peut avoir des exigences et des méthodologies différentes.

———————

Chapitre 2

NOTIONS FONDAMENTALES DE GESTION DE LA SÉCURITÉ

2.1 LE CONCEPT DE SÉCURITÉ ET SON ÉVOLUTION

2.1.1 Ce chapitre donne un aperçu des concepts et pratiques fondamentaux de gestion de la sécurité. Il importe de comprendre ces notions fondamentales avant de se concentrer sur les spécificités de la gestion de la sécurité abordées dans les chapitres subséquents.

2.1.2 Dans le contexte de l'aviation, la sécurité est « l'état dans lequel les risques liés aux activités aéronautiques concernant, ou appuyant directement, l'exploitation des aéronefs sont réduits et maîtrisés à un niveau acceptable ».

2.1.3 La sécurité de l'aviation est dynamique. De nouveaux dangers et risques apparaissent constamment et doivent être atténués. Tant que les risques de sécurité sont maintenus sous un niveau approprié de contrôle, la sécurité d'un système aussi ouvert et dynamique que l'est l'aviation peut encore être assurée. Il convient de noter que la performance de sécurité acceptable est souvent définie et influencée par les normes et la culture nationales et internationales.

2.1.4 Les avancées en matière de sécurité de l'aviation peuvent être décrites par quatre approches, correspondant dans les grandes lignes à des ères d'activités. Ces approches sont énumérées ci-dessous et illustrées à la Figure 2-1.

a) *L'ère 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 (l'aéronef, par exemple). 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'ère des facteurs humains* — 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 des facteurs humains, y compris à l'interface homme/machine. Malgré l'investissement de ressources dans l'atténuation des erreurs, la performance humaine continue d'être citée comme facteur récurrent d'accidents. 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 qu'au début des années 1990 qu'on a commencé à reconnaître que les individus opèrent dans un environnement complexe, qui inclut de multiples facteurs ayant le potentiel d'affecter le comportement.

c) *L'ère organisationnelle* — Vers le milieu des années 1990, la sécurité a commencé à être considérée dans une perspective systémique, englobant les facteurs organisationnels ainsi que les facteurs humains et techniques. Il en est résulté l'introduction de la notion d'« accident organisationnel », prenant en considération l'incidence de la culture et des politiques organisationnelles sur l'efficacité de

la maîtrise des risques de sécurité. De plus, la collecte et l'analyse régulières de données de sécurité à l'aide de méthodologies réactives et proactives ont permis aux organisations de surveiller les risques de sécurité connus et de détecter les tendances émergentes en matière de sécurité. Ces améliorations ont livré les leçons et les fondements à la base de l'approche actuelle de la gestion de la sécurité.

d) *Approche visant l'ensemble du système* — Dès le début du XXI^{e} siècle, de nombreux États et prestataires de services avaient fait leurs les approches de sécurité du passé et avaient atteint un niveau supérieur de maturité en matière de sécurité. Ils ont commencé à mettre en œuvre un PNS ou des SGS et en récoltent maintenant les fruits. Toutefois, les systèmes de sécurité en place à ce jour se concentrent surtout sur la performance de sécurité individuelle et sur la maîtrise à l'échelon local, en tenant peu compte du contexte général de l'ensemble du système aéronautique. De plus en plus d'acteurs reconnaissent aujourd'hui la complexité du système aéronautique et des différentes organisations qui jouent un rôle dans la sécurité de l'aviation. L'analyse de nombreux accidents et incidents montre que les interfaces entre organisations ont contribué à des résultats négatifs.

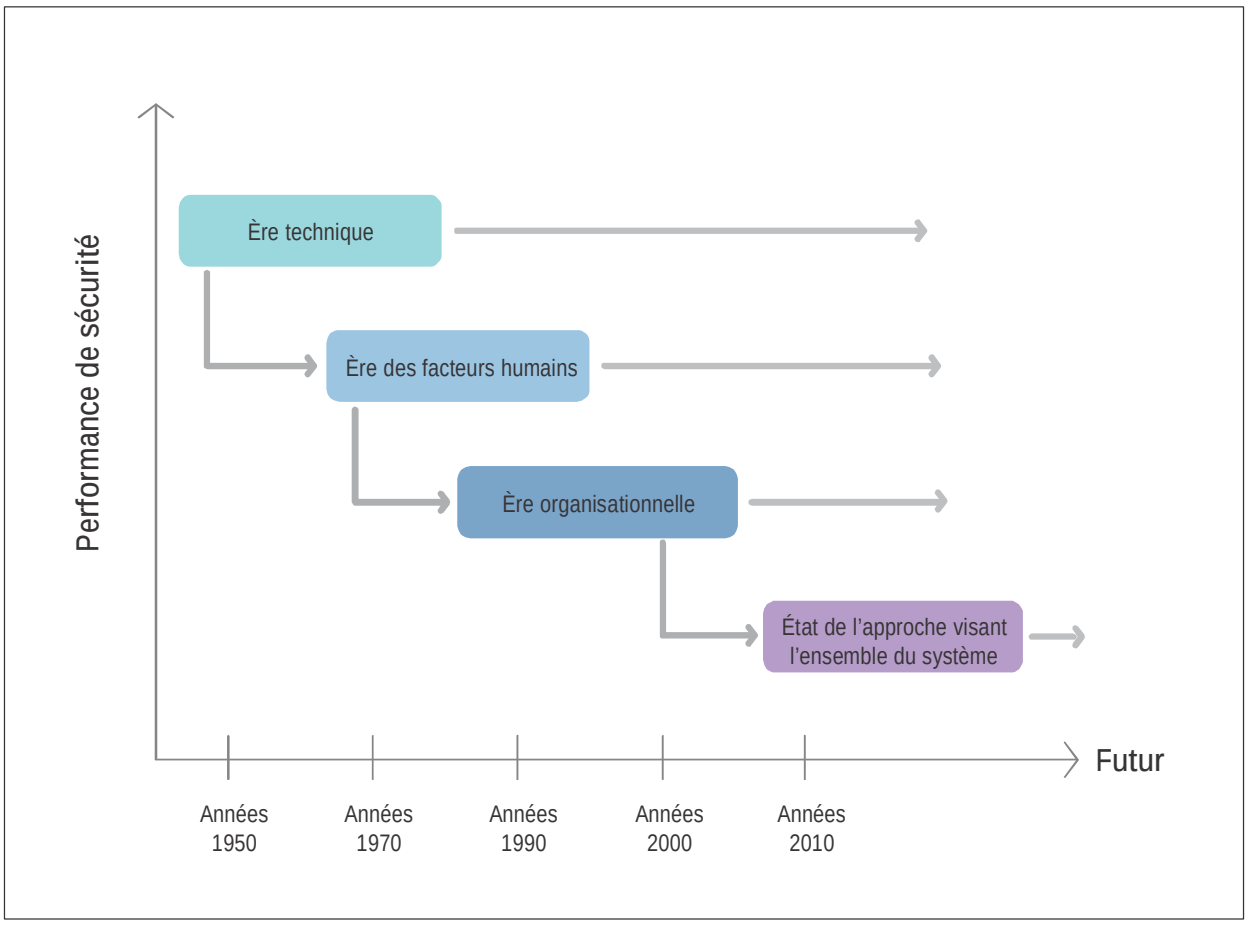

Figure 2-1. Évolution de la sécurité

2.1.5 L'évolution constante et cumulative de la sécurité a amené les États et les prestataires de services à sérieusement envisager les interactions et les interfaces entre les composants du système : les humains, les processus et les technologies. Ce travail a abouti à une meilleure appréciation du rôle positif des humains dans le système. La sécurité profite d'une collaboration entre les prestataires de services, et entre les prestataires de services et les États. Cette perspective a alimenté de multiples initiatives de collaboration entre prestataires de services et a généré une appréciation des avantages d'une collaboration dans la gestion des questions de sécurité. Le Programme de sécurité des pistes de l'OACI en est un bon exemple.

2.1.6 Pour qu'une approche collaborative visant l'ensemble du système puisse se développer, les interfaces et interactions entre les organisations (y compris les États) doivent être bien comprises et gérées. Les États commencent aussi à reconnaître le rôle que l'approche visant l'ensemble du système aéronautique peut jouer dans l'élaboration de leur PNS. Cette approche permet, par exemple, de gérer les risques de sécurité qui sont communs à de multiples activités aéronautiques.

2.2 LES HUMAINS DANS LE SYSTÈME

2.2.1 La façon dont les humains perçoivent leurs responsabilités en matière de sécurité et la façon dont ils interagissent avec d'autres pour exécuter leurs tâches au travail affectent considérablement la performance de sécurité de leur organisation. La gestion de la sécurité doit aborder la manière dont les humains contribuent, tant positivement que négativement, à la sécurité de l'organisation. Les facteurs humains visent à permettre de comprendre comment les humains interagissent avec le monde et quelles sont leurs capacités et limites, et à influencer l'activité humaine pour améliorer la façon dont les humains effectuent leur travail. En conséquence, la prise en considération des facteurs humains fait partie intégrante de la gestion de la sécurité et est nécessaire pour comprendre, identifier et atténuer les risques ainsi que pour optimiser les contributions humaines à la sécurité des organisations.

2.2.2 Les processus de gestion de la sécurité prennent en considération les facteurs humains principalement comme suit :

a) l'engagement de la haute direction à créer un environnement de travail qui optimise la performance humaine et encourage le personnel à prendre part et à contribuer activement aux processus de gestion de la sécurité de l'organisation ;

b) les responsabilités du personnel en matière de gestion de la sécurité sont clarifiées afin de garantir une compréhension et des attentes communes ;

c) l'organisation donne au personnel des informations qui :

   1) décrivent les comportements attendus en rapport avec les processus et procédures de l'organisation ;

   2) décrivent les actions qui seront entreprises par l'organisation en réaction aux comportements individuels ;

d) les niveaux de dotation en personnel sont surveillés et adaptés pour garantir la présence de suffisamment de personnes pour répondre aux besoins opérationnels ;

e) des politiques, processus et procédures sont établis pour encourager les comptes rendus de sécurité ;

f) les données de sécurité et les informations de sécurité sont analysées pour permettre la prise en considération des risques liés à la variabilité de la performance humaine et aux limites humaines, une attention particulière étant accordée à tout facteur organisationnel ou opérationnel qui y serait associé ;

g) des politiques, processus et procédures clairs, concis et applicables sont élaborés pour :

1) optimiser les performances humaines ;

2) prévenir des erreurs involontaires ;

3) réduire les conséquences non souhaitées de la variabilité de la performance humaine ; l'efficacité de ces politiques, processus et procédures est constamment surveillée en situation normale ;

h) le suivi permanent en situation normale inclut l'évaluation de l'application des processus et procédures et, en cas de non-application, la réalisation d'enquêtes pour en déterminer la cause ;

i) les enquêtes en matière de sécurité incluent l'évaluation des facteurs humains contributifs, évaluation qui examine non seulement les comportements mais aussi les raisons de ces comportements (contexte), étant entendu que, dans la plupart des cas, les humains font tout leur possible pour exécuter leurs tâches ;

j) la gestion des processus de changement inclut la prise en considération des tâches et rôles évolutifs des humains dans le système ;

k) des formations sont données au personnel afin de garantir que celui-ci est compétent pour exécuter ses tâches ; l'efficacité de la formation est analysée et les programmes de formation sont adaptés pour répondre à l'évolution des besoins.

2.2.3 L'efficacité de la gestion de la sécurité dépend en grande partie du degré de soutien de la haute direction et de l'engagement de la direction à créer un environnement de travail qui optimise la performance humaine et encourage le personnel à prendre part et à contribuer activement aux processus de gestion de la sécurité de l'organisation.

2.2.4 En ce qui concerne l'influence de l'organisation sur la performance humaine, il faut un appui de la haute direction pour mettre en œuvre une gestion efficace de la sécurité. Pour aborder les facteurs humains, la direction doit notamment s'engager à créer le bon environnement de travail et la bonne culture de la sécurité. Cela influencera aussi les attitudes et les comportements de tout un chacun au sein de l'organisation. De plus amples informations sur la culture de la sécurité figurent au Chapitre 3.

2.2.5 Plusieurs modèles ont été créés pour soutenir l'évaluation de l'influence des facteurs humains sur la performance de sécurité. Le modèle SHELL, bien connu, est utile pour illustrer l'incidence de l'interaction des différents composants du système sur l'humain et met en lumière la nécessité de considérer les facteurs humains comme une partie intégrante de la GRS.

2.2.6 La Figure 2-2 illustre la relation entre l'humain (au centre du modèle) et les composants du lieu de travail. Le modèle SHELL compte quatre composantes satellites :

a) *Software (S) :* procédures, formation, appui, etc. ;

b) *Hardware (H) :* machines et équipement ;

c) *Environment (E) :* environnement de travail dans lequel le reste du système L-H-S doit fonctionner ;

d) *Liveware (L) :* autres humains sur le lieu de travail.

Figure 2-2. Le modèle SHELL

2.2.7 *Liveware*. Au centre du modèle SHELL se trouvent les humains, en première ligne des opérations. Toutefois, de toutes les composantes de ce modèle, celle-ci est la moins prévisible et la plus sensible aux effets d'influences internes (faim, fatigue, motivation, etc.) et externes (température, lumière, bruit, etc.). 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. 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*. Les bords ondulés des cubes représentent le couplage imparfait de chacun des modules. Ce modèle est utile pour visualiser les interfaces suivantes entre les divers éléments du système d'aviation :

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. Elle prend en considération les aspects ergonomiques de l'utilisation des équipements par le personnel, les modes d'affichage des informations de sécurité, ainsi que les modes d'étiquetage et d'actionnement des commutateurs et leviers de commande permettant une utilisation logique et intuitive de ceux-ci.

b) *Liveware-Software (L-S)*. L'interface L-S est la relation entre l'humain et les systèmes d'appui qui se trouvent sur le lieu de travail, tels que règlements, manuels, listes de vérification, publications, processus et procédures, et logiciels. Cette interface couvre des aspects tels que la récence de l'expérience, la précision, le format et la présentation, le vocabulaire, la clarté et la symbologie. L-S porte sur les processus et procédures — la facilité avec laquelle ceux-ci peuvent être appliqués et compris.

c) *Liveware-Liveware (L-L)*. L'interface L-L représente les relations et interactions entre les humains sur le lieu de travail. Certaines de ces interactions se déroulent au sein de l'organisation (collègues, superviseurs, directeurs) mais beaucoup d'entre elles ont lieu entre des personnes provenant d'organisations différentes ayant des rôles distincts (contrôleurs de la circulation aérienne et pilotes,

pilotes et ingénieurs, etc.). Cette interface tient compte de l'importance des compétences de communication et compétences interpersonnelles ainsi que de la dynamique de groupe pour déterminer la performance humaine. 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 permis aux organisations d'étudier la performance des équipes dans la gestion des erreurs. Les relations entre le personnel et l'encadrement se situent également à cette interface, de même que la culture organisationnelle.

d) *Liveware-Environment (L-E)*. Cette interface concerne les relations entre l'être humain et l'environnement physique. Ce dernier inclut des paramètres tels que la température, la lumière ambiante, le bruit, les vibrations et la qualité de l'air. Cette interface tient aussi compte de facteurs environnementaux externes, tels que la météorologie, les infrastructures et le relief.

2.3 CAUSALITÉ DES ACCIDENTS

2.3.1 Le modèle du « fromage suisse » (ou modèle de Reason), élaboré par le professeur James Reason et bien connu dans l'industrie aéronautique, illustre le fait que les accidents découlent de violations successives de multiples mécanismes de défense. Ces violations peuvent être déclenchées par plusieurs facteurs contributifs, tels que des défaillances d'équipements ou des erreurs opérationnelles. Le modèle du fromage suisse affirme que des systèmes complexes tels que l'aviation sont extrêmement bien défendus par des couches de défenses (aussi appelées « barrières »). Une défaillance en un seul point est rarement grave. Des violations des défenses de sécurité peuvent être une conséquence tardive de décisions prises aux niveaux supérieurs de l'organisation, qui peuvent rester dormantes jusqu'à ce que leurs effets ou leur potentiel néfaste soient activés par certaines conditions d'exploitation (on parle de conditions latentes). Dans de telles circonstances spécifiques, les défaillances humaines (ou « défaillances actives ») au niveau opérationnel entraînent une violation des couches finales de défenses de sécurité. Selon le modèle de Reason, tous les accidents comportent une combinaison de défaillances actives et de conditions latentes.

2.3.2 Les défaillances actives sont des actions ou des inactions, y compris des erreurs et des violations de règles, qui ont un effet préjudiciable immédiat. Elles sont perçues, avec le bénéfice du recul, comme des actes dangereux. Les défaillances actives sont associées au personnel de première ligne (pilotes, contrôleurs aériens, techniciens de maintenance d'aéronefs, etc.) et peuvent entraîner un résultat dommageable.

2.3.3 Les conditions latentes peuvent être présentes dans le système bien avant un résultat dommageable. Les conséquences des conditions latentes peuvent prendre beaucoup de temps à se manifester. De prime abord, ces conditions latentes ne sont pas perçues comme préjudiciables mais, dans certaines circonstances, elles peuvent apparaître au grand jour lorsqu'il y a violation de défenses au niveau opérationnel. Des personnes très éloignées de l'événement à la fois dans le temps et dans l'espace peuvent créer ces conditions. Les conditions latentes dans le système peuvent inclure des conditions générées par la culture de la sécurité, des choix d'équipements ou des conceptions de procédures, des objectifs organisationnels conflictuels, des systèmes organisationnels défectueux, ou des décisions de la direction.

2.3.4 Le paradigme de « l'accident organisationnel » contribue à identifier ces conditions latentes à l'échelon du système, plutôt que par des efforts localisés, en vue de réduire au minimum les défaillances actives d'individus. Point important, les conditions latentes, lorsqu'elles ont été créées, répondaient à de bonnes intentions. Les décideurs des organisations recherchent souvent un équilibre entre ressources limitées, d'une part, et priorités potentiellement conflictuelles et coûts, d'autre part. Les décisions prises par les décideurs, sur une base quotidienne dans de grandes organisations, pourraient, dans des circonstances particulières, mener involontairement à un résultat dommageable.

2.3.5 La Figure 2-3 montre comment le modèle du fromage suisse permet de comprendre les interactions entre facteurs organisationnels et facteurs de gestion dans les causes des accidents. De multiples couches de défenses sont intégrées dans le système d'aviation pour assurer une protection contre des variations de la performance humaine ou contre des décisions à tous les niveaux de l'organisation. Toutefois, chaque couche a généralement des faiblesses, illustrées par les trous dans les tranches du « fromage suisse ». Parfois toutes ces faiblesses s'alignent (représentées par les trous alignés), ce qui entraîne une violation qui traverse toutes les barrières défensives et peut aboutir à un résultat catastrophique. Le modèle du fromage suisse montre que des conditions latentes sont toujours présentes dans le système et illustre comment elles peuvent se manifester par le biais de facteurs déclencheurs locaux.

2.3.6 Il est important de reconnaître que certaines des défenses, ou violations, peuvent être influencées par une organisation en interface. Il est dès lors crucial que les prestataires de services évaluent et gèrent ces interfaces.

2.3.7 Applications du « fromage suisse » à la gestion de la sécurité

2.3.7.1 Le modèle du « fromage suisse » peut être utilisé comme guide d'analyse tant par les États que par les prestataires de services pour examiner les circonstances organisationnelles qui, par-delà les individus concernés par un incident ou par un danger identifié, ont pu permettre à la situation de se manifester. Il peut être appliqué pendant la GRS, la surveillance de la sécurité, les audits internes, la gestion du changement et les enquêtes en matière de sécurité. Dans chaque cas, le modèle peut être utilisé pour déterminer quelles défenses de l'organisation sont efficaces et quelles défenses sont susceptibles d'être violées ou l'ont été, et pour évaluer l'utilité d'ajouter des défenses supplémentaires au système. Une fois identifiée, toute défense présentant des faiblesses peut être renforcée afin de prévenir de futurs accidents et incidents.

2.3.7.2 Concrètement, l'événement violera les défenses dans le sens de la flèche (des dangers vers les pertes), comme illustré à la Figure 2-3. Les évaluations de la situation seront effectuées dans le sens contraire, dans ce cas, des pertes vers les dangers. Des accidents d'aviation réels incluront généralement un certain degré de complexité supplémentaire. Il existe des modèles plus sophistiqués qui peuvent aider les États et les prestataires de services à comprendre comment et pourquoi des accidents se produisent.

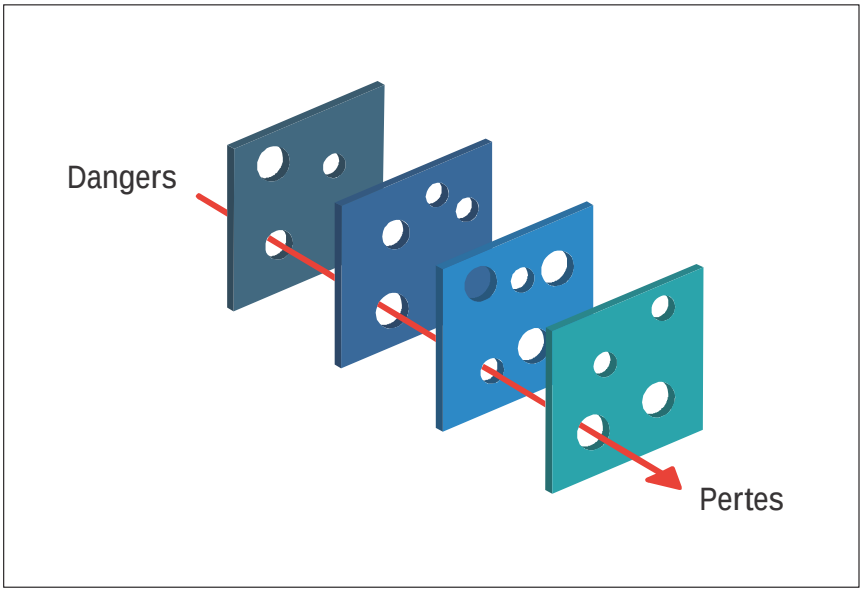

Figure 2-3. Concept de causalité des accidents

2.3.8 La dérive pratique

2.3.8.1 La théorie de la dérive pratique de Scott A. Snook est utilisée pour comprendre comment la performance de n'importe quel système « dérive » de sa conception d'origine. Les tâches, procédures et équipements sont souvent conçus et planifiés initialement dans un environnement théorique, dans des conditions idéales, avec pour hypothèse implicite que presque tout peut être prédit et maîtrisé, environnement dans lequel tout fonctionne comme prévu. Ce système initial repose sur trois hypothèses fondamentales :

a) la technologie nécessaire pour atteindre les objectifs de production du système est disponible ;

b) le personnel est formé, compétent et motivé pour utiliser la technologie correctement ;

c) la politique et les 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 partant du début du déploiement opérationnel du système, comme illustré à la Figure 2-4.

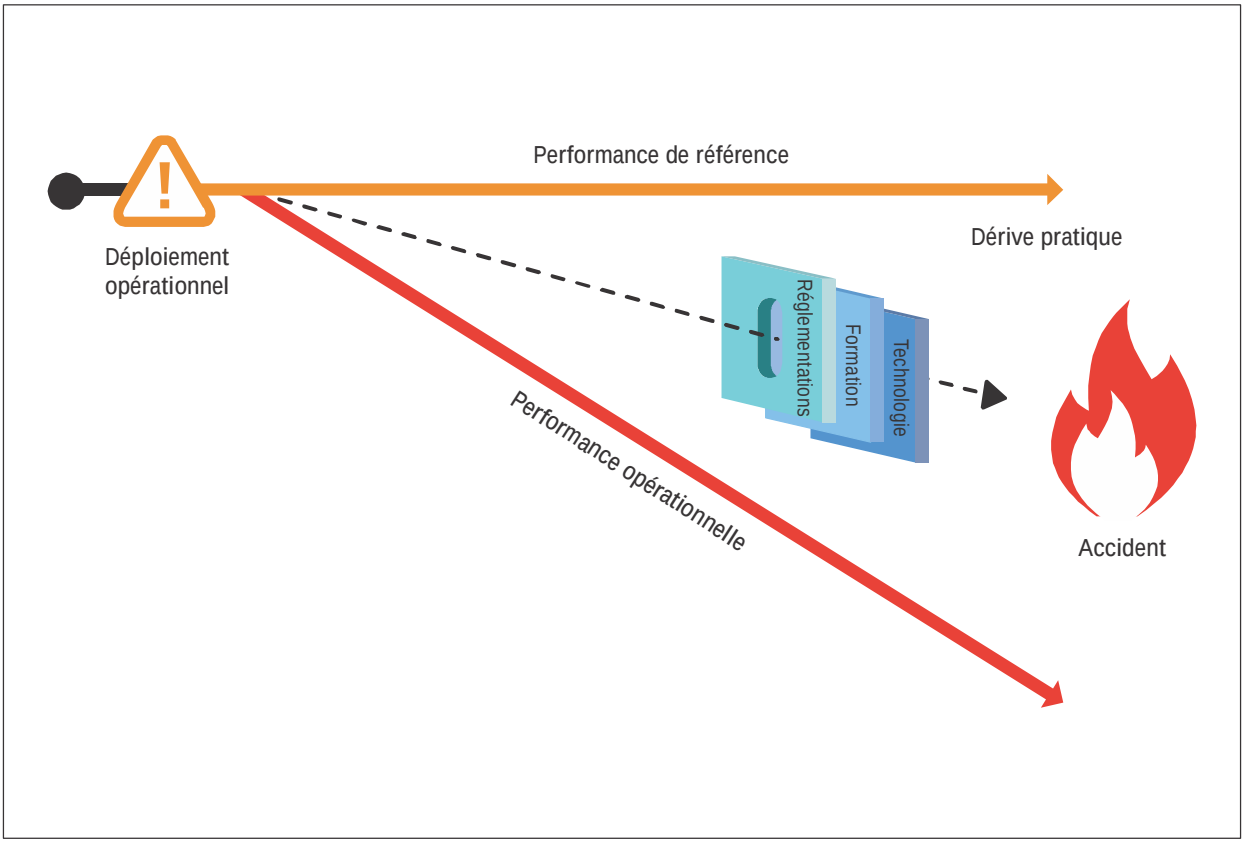

Figure 2-4. Concept de la dérive pratique

2.3.8.2 Une fois déployé de façon opérationnelle, le système devrait idéalement fonctionner comme il a été conçu, la plupart du temps selon la performance de référence (ligne orange). En réalité, la performance opérationnelle diffère souvent de la performance de référence présumée, en conséquence des opérations dans la vie réelle, qui se déroulent dans un environnement complexe, généralement exigeant et en perpétuelle mutation (ligne rouge). 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.

2.3.8.3 M. Snook affirme que la dérive pratique est inévitable dans tout système, si minutieuse et réfléchie qu'ait été la conception de ce dernier. Voici quelques raisons d'une dérive pratique :

a) une technologie qui ne fonctionne pas comme prévu ;

b) des procédures qui, dans certaines circonstances opérationnelles, ne peuvent pas être exécutées comme cela a été planifié ;

c) l'introduction de changements dans le système, notamment l'ajout de nouveaux éléments ;

d) les interactions avec d'autres systèmes ;

e) la culture de la sécurité ;

f) l'adéquation (ou inadéquation) des ressources (p. ex. équipement d'appui) ;

g) les leçons tirées des succès et des échecs pour améliorer les opérations, etc.

2.3.8.4 Le fait demeure cependant que, en dépit de toutes les insuffisances du système, les humains font généralement fonctionner le système quotidiennement, en appliquant des adaptations locales (ou contournements) et des stratégies personnelles. Ces contournements peuvent court-circuiter la protection offerte par les mécanismes existants de défense et de maîtrise des risques de sécurité.

2.3.8.5 Les activités d'assurance de la sécurité telles que les audits, les observations et le suivi des SPI peuvent contribuer à mettre au jour des activités relevant de la « dérive pratique ». Analyser les informations de sécurité pour déterminer pourquoi la dérive se produit permet d'atténuer les risques de sécurité. Plus rapidement la dérive pratique sera détectée après le début du déploiement opérationnel, plus il sera facile pour l'organisation d'intervenir. De plus amples informations sur l'assurance de la sécurité pour les États et les prestataires de services figurent aux Chapitres 8 et 9, respectivement.

2.4 LE DILEMME DE LA GESTION

2.4.1 Dans toute organisation pratiquant la prestation de services, production/rentabilité et risques de sécurité sont liés. Une organisation doit maintenir sa rentabilité pour rester en activité, en cherchant un équilibre entre production et risques de sécurité acceptables (et les coûts découlant de la mise en œuvre de mesures de maîtrise des risques de sécurité). Les mesures classiques de maîtrise des risques de sécurité reposent sur la technologie, la formation, les processus et les procédures. Pour l'État, les mesures de maîtrise des risques de sécurité sont similaires, à savoir la formation du personnel, l'utilisation appropriée de la technologie, une supervision efficace et des processus et procédures internes à l'appui de la supervision. La mise en œuvre de mesures de maîtrise des risques de sécurité a un coût — en termes d'argent, de temps et de ressources — et le but de ces mesures est généralement d'améliorer la performance de sécurité et non la performance de production. Néanmoins, certains investissements dans la « protection » peuvent aussi améliorer la « production » en réduisant les accidents et les incidents et, par conséquent, les coûts qui y sont associés.

2.4.2 L'espace de sécurité est une métaphore décrivant la zone au sein de laquelle une organisation recherche un équilibre entre la production/rentabilité souhaitée et le maintien de la protection de la sécurité nécessaire au moyen de mesures de maîtrise des risques de sécurité. Par exemple, un prestataire de services pourrait souhaiter investir dans de nouveaux équipements. Ces nouveaux équipements peuvent apporter simultanément les améliorations de l'efficience 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 pour l'organisation et une évaluation des risques de sécurité connexes. Affecter des ressources excessives à des mesures de maîtrise des risques de sécurité pourrait avoir pour résultat que l'activité devienne non rentable, ce qui compromettrait la viabilité de l'organisation.

2.4.3 D'un autre côté, l'attribution de ressources excessives à la production, aux dépens de la protection, pourrait avoir une incidence sur le produit ou le service 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'un déséquilibre est en train de se développer ou existe déjà dans l'affectation des ressources. Les organisations utilisent des systèmes de gestion financière pour reconnaître quand elles sont trop près de la faillite et, en matière de gestion de la sécurité, appliquent la même logique et les mêmes outils pour surveiller leur performance de sécurité. Cela permet à l'organisation de fonctionner de façon rentable et sûre dans les limites de l'espace de sécurité. La Figure 2-5 présente une illustration des limites de l'espace de sécurité d'une organisation. Les organisations doivent constamment surveiller et gérer leur espace de sécurité car les risques de sécurité et les influences externes évoluent au fil du temps.

2.4.4 La nécessité de trouver un équilibre entre rentabilité et sécurité (ou production et protection) est devenue une exigence aisément comprise et acceptée par les prestataires de services. Cet équilibre est également applicable à la gestion de la sécurité par l'État, vu le besoin d'équilibrer les ressources nécessaires pour les fonctions étatiques de protection, qui incluent la certification et la surveillance.

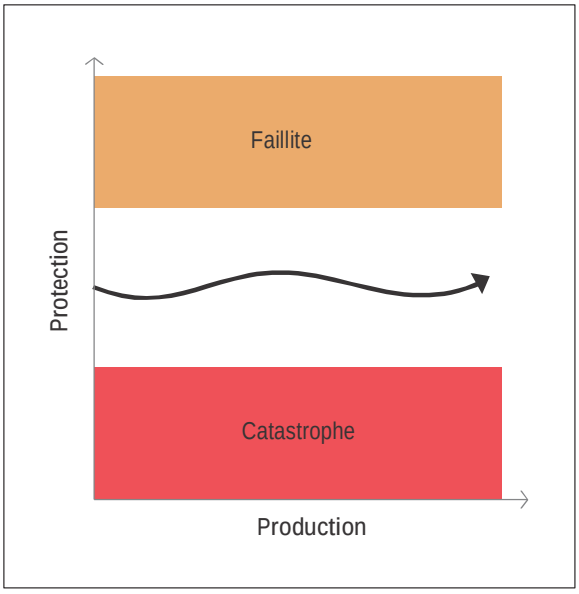

Figure 2-5. Concept de l'espace de sécurité

2.5 GESTION DES RISQUES DE SÉCURITÉ

La gestion des risques de sécurité (GRS) est un élément clé de la gestion de la sécurité et inclut l'identification des dangers, l'évaluation des risques de sécurité, l'atténuation des risques de sécurité et l'acceptation des risques. La GRS est une activité permanente parce que le système d'aviation évolue constamment, que de nouveaux dangers peuvent être introduits et que certains dangers et les risques de sécurité qui y sont associés peuvent changer au fil du temps. De plus, il faut surveiller l'efficacité des stratégies d'atténuation des risques de sécurité mises en œuvre afin de déterminer si de nouvelles actions sont requises.

2.5.1 Introduction sur les dangers

2.5.1.1 En aviation, un danger peut être considéré comme recelant un potentiel dormant de causer préjudice, présent sous une forme ou une autre dans le système ou dans son environnement. Ce potentiel de causer préjudice peut se manifester sous diverses formes, par exemple, comme une circonstance naturelle (p. ex. le relief) ou un état technique (p. ex. les marques de piste).

2.5.1.2 Les dangers font inévitablement partie des activités d'aviation mais leurs manifestations et leurs conséquences néfastes possibles peuvent être limitées par l'application de diverses stratégies d'atténuation visant à réduire la possibilité qu'un danger aboutisse à une situation dangereuse. L'aviation peut coexister avec des dangers pour autant que ceux-ci soient maîtrisés. L'identification des dangers est la première étape du processus de GRS. Elle précède une évaluation des risques de sécurité et requiert une compréhension claire des dangers et de leurs conséquences.

2.5.2 Comprendre les dangers et leurs conséquences

2.5.2.1 L'identification des dangers se concentre sur les situations ou sur les objets ayant le potentiel de causer ou de contribuer à causer un fonctionnement dangereux de l'aéronef ou d'équipements, de produits et de services en rapport avec la sécurité de l'aviation (les paragraphes suivants donnent des indications sur la distinction entre dangers directement pertinents pour la sécurité de l'aviation et autres dangers généraux/industriels).

2.5.2.2 Considérons, par exemple, un vent de 15 nœuds. Un vent de 15 nœuds n'est pas nécessairement une situation 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 crée une condition de vent traversier qui peut être dangereuse pour l'exploitation, du fait de son potentiel de contribuer à une instabilité de l'aéronef. La diminution de la maîtrise pourrait provoquer un événement tel qu'une sortie latérale de piste.

2.5.2.3 On a souvent tendance à confondre les dangers avec leurs conséquences. Une conséquence est un résultat qui peut être 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. Définir d'abord clairement le danger permettra de déterminer plus facilement les conséquences possibles.

2.5.2.4 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. 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 des risques de sécurité identifient toutes les conséquences possibles. La conséquence la plus extrême, la perte de vie humaine, devrait être différenciée des situations comportant des conséquences moindres, telles que des incidents d'aéronef, une charge de travail accrue pour l'équipage de conduite ou un inconfort pour les passagers. La description des conséquences facilitera l'évaluation des risques et l'élaboration et la mise en œuvre subséquentes de stratégies d'atténuation par une priorisation et une affectation de ressources. Une identification détaillée et complète des dangers permettra une évaluation plus précise des risques de sécurité.

Identification et priorisation des dangers

2.5.2.5 Des dangers existent à tous les niveaux de l'organisation et peuvent être détectés par de nombreux moyens, notamment des systèmes de compte rendu, des inspections, des audits, des sessions de recherche d'idées et l'appréciation d'experts. Le but est d'identifier proactivement les dangers avant que ceux-ci ne causent des accidents, des incidents ou d'autres événements liés à la sécurité. Un mécanisme important d'identification proactive des dangers est un système de compte rendu volontaire en matière de sécurité. Le Chapitre 5 contient de plus amples indications sur les systèmes de compte rendu volontaire en matière de sécurité. Les informations recueillies au moyen de tels systèmes de compte rendu peuvent être complétées par des observations ou des constatations enregistrées pendant des inspections régulières sur place ou des audits de l'organisation.

2.5.2.6 Les dangers peuvent aussi être identifiés à partir de l'examen ou de l'étude de comptes rendus d'enquêtes internes et externes. Une prise en considération des dangers dans l'analyse des rapports d'enquêtes sur les accidents/incidents est un bon moyen pour renforcer le système d'identification des dangers d'une organisation. Elle est particulièrement importante dans les organisations où la culture de la sécurité n'est pas suffisamment à maturité pour soutenir un système efficace de compte rendu volontaire en matière de sécurité, ou dans de petites organisations où le nombre d'événements ou de comptes rendus est limité. Des sources externes telles que l'OACI, des associations professionnelles ou d'autres organismes internationaux peuvent livrer d'importantes informations sur les dangers spécifiques liés à l'exploitation et aux activités.

2.5.2.7 L'identification des dangers peut aussi envisager les dangers générés en dehors de l'organisation et les dangers qui échappent au contrôle direct de l'organisation, tels que des conditions météorologiques extrêmes ou des cendres volcaniques. Les dangers liés aux risques de sécurité émergents sont aussi, pour les organisations, un mode de préparation important à des situations qui pourraient finir par se produire.

2.5.2.8 Il convient de prendre en compte les éléments suivants dans le cadre du processus d'identification des dangers :

a) la description du système ;

b) les facteurs de conception, y compris la conception de l'équipement et des tâches ;

c) les limites des performances humaines (p. ex. limites physiologiques, psychologiques, physiques et cognitives) ;

d) les procédures et les pratiques d'exploitation, y compris la documentation et les listes de vérification, ainsi que leur validation en conditions d'exploitation réelles ;

e) les facteurs de la communication, y compris les médias, la terminologie et la langue ;

f) les facteurs organisationnels, tels que ceux qui sont liés au recrutement, à la formation et à la fidélisation du personnel, la compatibilité entre les objectifs de production et les objectifs de sécurité, l'affectation des ressources, les pressions de l'exploitation et la culture de la sécurité de l'entreprise ;

g) les facteurs liés à l'environnement opérationnel (p. ex. la météorologie, le bruit ambiant et les vibrations, la température et l'éclairage) ;

h) les facteurs de supervision réglementaire, y compris le champ d'application des règlements et leur force exécutoire, la certification de l'équipement, du personnel et des procédures ;

i) les systèmes de suivi des performances qui peuvent détecter la dérive pratique, les écarts opérationnels ou une détérioration de la fiabilité d'un produit ;

j) les facteurs concernant l'interface humain-machine ;

k) les facteurs liés aux interfaces PNS/SGS avec d'autres organisations.

Dangers pour la sécurité, la santé et l'environnement professionnels

2.5.2.9 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 composites. Un exemple de danger composite 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 composites n'étant pas les mêmes au niveau OSHE et au niveau de la sécurité de l'aviation, il convient de les envisager séparément. La finalité et la focalisation des contrôles préventifs pourraient être différentes pour les conséquences OSHE et pour les conséquences en matière de sécurité de l'aviation.

Méthodes d'identification des dangers

2.5.2.10 Il existe deux méthodes principales 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 enquêtes sur les événements de sécurité. Les incidents et accidents sont des indicateurs de carences du système et peuvent donc être utilisés pour déterminer le ou les dangers ayant contribué à l'événement.

b) *Proactive*. Cette méthode consiste à collecter des données de sécurité provenant d'événements aux conséquences mineures ou des données sur la performance des processus et à analyser les informations de sécurité ou la fréquence des événements afin de déterminer si un danger pourrait entraîner un accident ou un incident. Les informations de sécurité pertinentes pour l'identification proactive des dangers proviennent de programmes d'analyse des données de vol (FDA), de systèmes de compte rendu de sécurité et de la fonction d'assurance de la sécurité.

2.5.2.11 L'analyse des données de sécurité permet aussi d'identifier des dangers en détectant des tendances négatives et en formulant des prévisions sur les dangers émergents, etc.

Dangers liés aux interfaces des SGS avec des organisations externes

2.5.2.12 Les organisations devraient aussi identifier les dangers liés aux interfaces de leur gestion de la sécurité. Elles devraient, dans la mesure du possible, effectuer ce travail en tant qu'exercice conjoint avec les organisations en interface. L'identification des dangers devrait étudier l'environnement opérationnel et les diverses capacités organisationnelles (humains, processus, technologies) susceptibles de contribuer à une prestation sûre du service ou à la disponibilité du produit, à sa fonctionnalité ou à sa performance.

2.5.2.13 À titre d'exemple, beaucoup d'organisations et de personnels opérationnels, actifs dans et autour de l'aéronef, jouent un rôle dans le temps d'escale d'un aéronef. Des dangers sont susceptibles d'apparaître aux interfaces entre le personnel d'exploitation, les équipements utilisés et la coordination de l'activité liée au temps d'escale.

2.5.3 Probabilité des risques de sécurité

2.5.3.1 La probabilité des risques de sécurité est définie comme la probabilité d'occurrence d'une conséquence ou d'un résultat en matière de sécurité. Il est important d'envisager une série de scénarios de façon à ce que toutes les conséquences potentielles puissent être prises en compte. Les questions suivantes peuvent aider à déterminer la probabilité :

a) Existe-t-il un historique d'occurrences similaires à celle qui est en cours d'examen ou s'agit-il d'un cas isolé ?

b) D'autres équipements ou éléments du même type pourraient-ils présenter des défectuosités semblables ?

c) Au sein du personnel, quel est le nombre de personnes qui appliquent les procédures considérées ou qui y sont soumises ?

d) Quelle est l'exposition au danger envisagé ? Par exemple, pendant quel pourcentage du temps de l'opération l'équipement est-il utilisé ou l'activité est-elle pratiquée ?

2.5.3.2 La prise en considération de tous les facteurs qui pourraient sous-tendre ces questions aidera à évaluer la probabilité des conséquences du danger dans tous les scénarios prévisibles.

2.5.3.3 Un événement est considéré comme prévisible si toute personne raisonnable avait pu prévoir que ce type d'événement se produirait dans les mêmes circonstances. Il n'est pas possible d'identifier tous les dangers imaginables ou théoriquement possibles. Par conséquent, il faut faire preuve de discernement pour déterminer le niveau de détail approprié à appliquer à l'identification des dangers. Les prestataires de services devraient faire preuve de diligence raisonnable lorsqu'ils identifient des dangers significatifs et raisonnablement prévisibles liés à leur produit ou service.

Note.— En ce qui concerne la conception du produit, le terme « prévisible » est censé être compatible avec son utilisation dans les règlements de navigabilité, les politiques et les conseils.

2.5.3.4 Le Tableau 1 présente une classification type de la probabilité des risques de sécurité. Il comporte 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. Cet exemple utilise des termes qualitatifs. Des termes quantitatifs pourraient être définis pour fournir une évaluation plus précise. Cela dépendra de la disponibilité de données de sécurité appropriées et de la sophistication de l'organisation et de l'exploitation.

Tableau 1. Tableau de probabilité des risques de sécurité

Probabilité	*Signification*	*Valeur*
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
Faible	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

Note.— Ceci n'est qu'un simple exemple. Le niveau de détail et la complexité des tableaux et des matrices devraient être adaptés aux besoins particuliers et à la complexité de chaque organisation. Il est à noter aussi que les organisations peuvent inclure à la fois des critères qualitatifs et des critères quantitatifs.

2.5.4 Gravité d'un risque de sécurité

2.5.4.1 Une fois achevée l'évaluation de la 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. La classification de la gravité devrait tenir compte des éléments suivants :

a) les pertes de vies humaines ou les blessures graves qui surviendraient du fait :

   1) de la présence dans l'aéronef ;

   2) du contact direct avec une partie quelconque de l'aéronef, y compris avec des parties qui s'en sont détachées ; ou

   3) de l'exposition directe au souffle des réacteurs ; et

b) les dommages :

   1) dommages ou défaillances structurelles subis par l'aéronef :

      i) qui altèrent ses caractéristiques de résistance structurelle, de performance ou de vol ;

      ii) qui normalement devraient nécessiter une réparation importante ou le remplacement de l'élément endommagé ;

   2) dommages subis par les ATS ou les équipements d'un aérodrome :

      i) qui ont une incidence négative sur la gestion de la séparation des aéronefs ; ou

      ii) qui ont une incidence négative sur la capacité d'atterrissage.

2.5.4.2 L'évaluation de la gravité devrait envisager toutes les conséquences possibles d'un danger, en tenant compte de la situation la plus défavorable prévisible. Le Tableau 2 présente une classification type de la gravité des risques de sécurité. Il comprend cinq catégories destinées à indiquer le niveau de gravité, la description de chaque catégorie et l'attribution d'une valeur à chaque catégorie. Comme pour le tableau de probabilité des risques de sécurité, ce tableau est un simple exemple.

Tableau 2. Exemple de classification de la gravité des risques de sécurité

Gravité	*Signification*	*Valeur*
Catastrophique	• Aéronef/équipement détruit • Multiples décès	A
Dangereux	• Importante réduction des marges de sécurité, détresse physique ou charge de travail telle qu'il n'est pas sûr que les opérateurs pourront accomplir leurs tâches de façon exacte ou complète	B

Gravité	*Signification*	*Valeur*
	• Blessures graves • Importants dommages aux équipements	
Majeur	• Importante réduction des marges de sécurité, réduction de la capacité des opérateurs à faire face à des conditions de travail défavorables, du fait d'une augmentation de la charge de travail ou en raison de conditions compromettant leur efficacité • Incident grave • Personnes blessées	C
Mineur	• Nuisance • Limites de fonctionnement • Recours à des procédures d'urgence • Incident mineur	D
Négligeable	• Peu de conséquences	E

2.5.5 Tolérabilité des risques de sécurité

2.5.5.1 L'indice de risque de sécurité est créé à partir des résultats des scores de probabilité et de gravité. Dans l'exemple ci-dessus, il s'agit d'un code alphanumérique. Les combinaisons gravité/probabilité respectives sont présentées dans la matrice d'évaluation des risques de sécurité au Tableau 3. Cette matrice sert à déterminer la tolérabilité du risque de sécurité. Prenons, par exemple, une situation où un risque de sécurité a été évalué comme Occasionnel (4), pour ce qui est de la probabilité, et comme Dangereux (B), en ce qui concerne la gravité, ce qui donne un indice de risque de sécurité de (4B).

Tableau 3. Exemple de matrice d'évaluation des risques de sécurité

Risque de sécurité		*Gravité*				
Probabilité		*Catastrophique A*	*Dangereux B*	*Majeur C*	*Mineur D*	*Négligeable E*
Fréquent	5	5A	5B	5C	5D	5E
Occasionnel	4	4A	4B	4C	4D	4E
Faible	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extrêmement improbable	1	1A	1B	1C	1D	1E

Note.— Pour déterminer la tolérabilité du risque de sécurité, il faut tenir compte de la qualité et de la fiabilité des données utilisées pour l'identification des dangers et de la probabilité du risque de sécurité.

2.5.5.2 L'indice obtenu à partir de la matrice d'évaluation des risques de sécurité devrait ensuite être exporté vers un tableau de tolérabilité du risque de sécurité qui décrit — sous forme narrative — les critères de tolérabilité pour l'organisation en question. Le Tableau 4 présente un exemple de tableau de tolérabilité des risques de sécurité. Dans l'exemple ci-dessus, le critère de risque de sécurité évalué en tant que 4B relève de la catégorie « intolérable ». Dans ce cas, l'indice de risque de sécurité de la conséquence est inacceptable. L'organisation devrait donc prendre des mesures de maîtrise des risques afin de réduire :

a) l'exposition de l'organisation au risque particulier, c'est-à-dire réduire la composante de probabilité du risque à un niveau acceptable ;

b) la gravité des conséquences liées au danger, c'est-à-dire réduire la composante de gravité du risque à un niveau acceptable ; ou

c) à la fois la gravité et la probabilité, de façon à ce que le risque soit géré à un niveau acceptable.

2.5.5.3 Les risques de sécurité sont évalués conceptuellement comme étant acceptables, tolérables ou intolérables. Les risques de sécurité qui sont évalués comme appartenant initialement au groupe des risques intolérables sont inacceptables dans toutes les circonstances. La probabilité et/ou la gravité des conséquences des dangers sont d'une telle ampleur et le potentiel de préjudice du danger constitue une telle menace pour la sécurité que des mesures d'atténuation doivent être impérativement adoptées ou les activités doivent être interrompues.

Tableau 4. Exemple de tolérabilité des risques de sécurité

Plage de l'indice de risque de sécurité	*Description du risque de sécurité*	*Mesure recommandée*
5A, 5B, 5C, 4A, 4B, 3A	INTOLÉRABLE	Adopter des mesures immédiates pour atténuer le risque ou arrêter l'activité. Réaliser une atténuation prioritaire des risques de sécurité afin de garantir que des contrôles préventifs additionnels ou renforcés sont en place pour abaisser l'indice des risques de sécurité à un niveau tolérable.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	TOLÉRABLE	Peut être toléré en fonction de l'atténuation des risques de sécurité. Cela peut nécessiter une décision de la direction en ce qui concerne l'acceptation du risque.
3E, 2D, 2E, 1B, 1C, 1D, 1E	ACCEPTABLE	Acceptable en l'état. Aucune autre mesure d'atténuation du risque n'est nécessaire.

2.5.6 Évaluation des risques liés aux facteurs humains

2.5.6.1 La prise en compte des facteurs humains revêt une importance particulière en GRS car les humains peuvent être à la fois une source de risques de sécurité et une solution à ces risques en :

a) contribuant à un accident ou à un incident par une performance variable due aux limites humaines ;

b) anticipant et en prenant des mesures appropriées pour éviter une situation dangereuse ;

c) résolvant des problèmes, prenant des décisions et prenant des mesures pour atténuer les risques.

2.5.6.2 Il est donc important de faire participer des personnes ayant les compétences appropriées en facteurs humains à l'identification, à l'évaluation et à l'atténuation des risques.

2.5.6.3 La GRS exige une prise en considération de tous les aspects des risques de sécurité, y compris ceux qui sont liés aux humains. L'évaluation des risques associés aux performances humaines est plus complexe que celle des facteurs de risque liés à la technologie et à l'environnement car :

a) la performance humaine est hautement variable, en fonction de l'interaction d'un large éventail d'influences internes et externes à l'individu. Nombre des effets de l'interaction entre ces influences sont difficiles, voire impossibles, à prédire ;

b) les conséquences de la variabilité de la performance humaine différeront selon la tâche effectuée et selon le contexte.

2.5.6.4 Cela complique le mode de détermination de la probabilité et de la gravité du risque. En conséquence, une maîtrise des facteurs humains est précieuse pour identifier et évaluer les risques de sécurité. (La gestion de la fatigue par le biais de processus de SGS est abordée dans le *Manuel pour la supervision des approches de gestion de la fatigue* [Doc 9966]).

2.5.7 Stratégies d'atténuation des risques de sécurité

2.5.7.1 L'atténuation des risques de sécurité est souvent appelée maîtrise des risques de sécurité. On devrait amener les risques de sécurité à un niveau acceptable en les atténuant par l'application de mesures appropriées de maîtrise des risques. Il faut trouver un juste équilibre entre le temps, le coût et la difficulté de prendre des mesures pour réduire ou éliminer le risque de sécurité. Il est possible de diminuer le niveau d'un risque de sécurité en réduisant la gravité de ses conséquences potentielles, la probabilité d'un événement ou l'exposition à ce risque de sécurité. Il est plus aisé et plus courant de réduire la probabilité que de réduire la gravité.

2.5.7.2 Les mesures d'atténuation des risques de sécurité sont des actions qui entraînent souvent des modifications des procédures opérationnelles, des équipements ou des infrastructures. Les stratégies d'atténuation des risques de sécurité se répartissent en trois catégories :

a) *Évitement :* L'opération ou l'activité est annulée ou évitée parce que le risque de sécurité est supérieur aux avantages à tirer de la poursuite de l'activité, ce qui élimine complètement le risque de sécurité.

b) *Réduction :* La fréquence de l'opération ou de l'activité est réduite ou des mesures sont prises pour réduire l'ampleur des conséquences du risque de sécurité.

c) *Ségrégation :* Des mesures sont prises pour isoler les effets des conséquences du risque de sécurité ou pour instaurer une redondance afin de se protéger contre ces effets.

2.5.7.3 La prise en compte des facteurs humains fait partie intégrante de l'identification des mesures efficaces d'atténuation parce que les humains doivent appliquer les mesures d'atténuation ou les mesures correctrices ou doivent y contribuer. Par exemple, des mesures d'atténuation peuvent inclure l'utilisation de processus ou de procédures. Sans la participation de ceux qui utiliseront ces mesures dans des situations de la « vie réelle » et/ou sans la participation de personnes expertes en facteurs humains, les processus ou procédures élaborés pourraient ne pas être adaptés et pourraient entraîner des conséquences involontaires. De plus, les limites des performances humaines devraient être prises en considération dans toute mesure d'atténuation du risque de sécurité et il faudrait intégrer des stratégies de capture des erreurs pour tenir compte de la variabilité des performances humaines. À terme, cette importante prise en considération des facteurs humains permet une atténuation plus efficace et plus complète.

2.5.7.4 Une stratégie d'atténuation des risques de sécurité 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 maîtrise possibles pour trouver une solution optimale. Il est nécessaire d'évaluer l'efficacité de chaque option particulière avant de prendre une décision. Chaque option d'atténuation des risques proposée devrait être examinée sous les angles suivants :

a) *Efficacité*. Mesure dans laquelle les options réduisent ou éliminent les risques de sécurité. L'efficacité peut être déterminée en fonction des moyens de défense techniques, didactiques et réglementaires qui peuvent réduire ou éliminer les risques de sécurité.

b) *Coût-avantage*. Mesure dans laquelle les avantages perçus de l'atténuation l'emportent sur les coûts.

c) *Faisabilité*. Mesure dans laquelle l'atténuation peut être mise en œuvre et est pertinente sur le plan de la technologie disponible, des ressources financières et administratives, de la législation, de la volonté politique, des réalités opérationnelles, etc.

d) *Acceptabilité*. Mesure dans laquelle l'option est acceptable pour ceux qui devront l'appliquer.

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 de sécurité.

h) *Conséquences involontaires.* L'introduction de nouveaux dangers et de risques de sécurité connexes associés à la mise en œuvre de toute solution d'atténuation.

i) *Temps*. Le temps requis pour mettre en œuvre la solution d'atténuation du risque de sécurité.

2.5.7.5 Toute action correctrice devrait tenir compte de tout moyen de défense existant et de la capacité ou de l'incapacité dudit moyen à maintenir un niveau acceptable de risque de sécurité. À cette fin, il se peut qu'il faille examiner les évaluations précédentes des risques de sécurité à la lumière de l'action correctrice appliquée. Les mesures d'atténuation et de maîtrise des risques de sécurité devront être vérifiées/soumises à audit pour garantir leur efficacité. Il est aussi possible d'assurer le suivi de l'efficacité des mesures d'atténuation par le biais des SPI. De plus amples informations sur la gestion des performances de sécurité et sur les SPI sont données au Chapitre 4.

2.5.8 Documentation de la gestion des risques de sécurité

2.5.8.1 Les activités de gestion des risques de sécurité devraient être documentées, notamment toute hypothèse sous-tendant l'évaluation de la probabilité et de la gravité, les décisions prises et toute mesure prise pour atténuer le

risque de sécurité. Pour ce faire, un tableur ou un tableau peut être utilisé. Certaines organisations peuvent utiliser une base de données ou d'autres logiciels dans lesquels de grandes quantités de données de sécurité et d'informations de sécurité peuvent être stockées et analysées.

2.5.8.2 La tenue à jour d'un registre des dangers identifiés réduit au minimum la probabilité que l'organisation perde de vue ses dangers connus. Lorsque des dangers sont identifiés, il est possible de les comparer à des dangers connus mentionnés dans le registre pour savoir si ce danger a déjà été enregistré et quelles actions ont été prises pour l'atténuer. Les registres de dangers sont généralement établis sous forme de tableaux et incluent le danger, les conséquences potentielles, l'évaluation des risques associés, la date d'identification, la catégorie de danger, une brève description, le moment ou le lieu où apparaît ce danger, qui l'a identifié et quelle mesure a été mise en place pour atténuer les risques.

2.5.8.3 Des outils et processus décisionnels concernant les risques de sécurité peuvent être utilisés pour améliorer la reproductibilité et la justification des décisions prises par les responsables de la sécurité de l'organisation. Un exemple d'aide à la prise de décision en matière de risque de sécurité est présenté ci-dessous, dans la Figure 2-6.

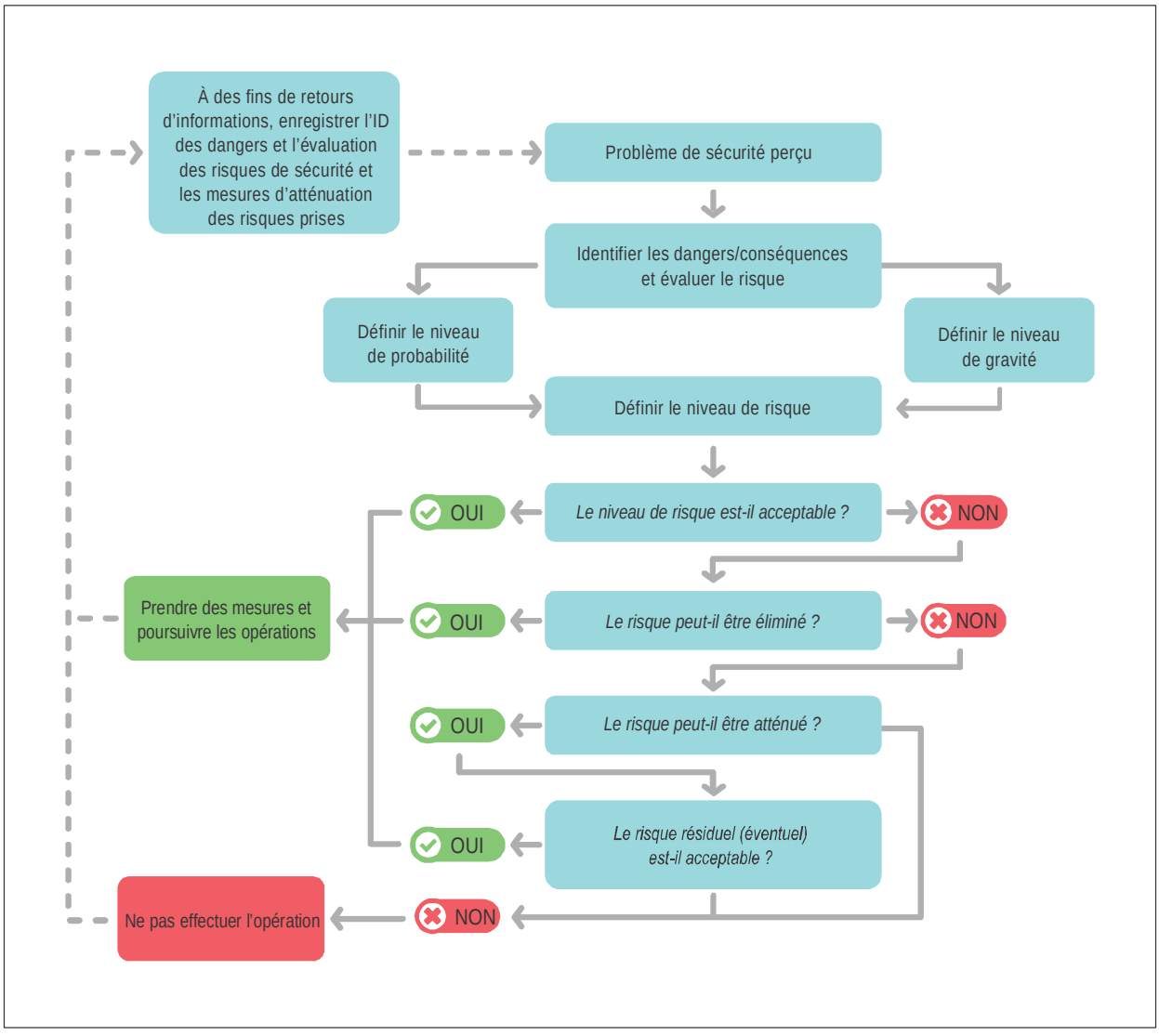

Figure 2-6. Aide à la décision en matière de gestion des risques de sécurité

2.5.9 Analyse coûts-avantages

L'analyse coûts-avantages ou coût-efficacité est normalement effectuée pendant les activités d'atténuation des risques de sécurité. Elle est communément associée à des processus de gestion, tels que des processus d'évaluation de l'incidence des réglementations ou des processus de gestion de projets. Dans certaines situations, cependant, une évaluation des risques de sécurité peut avoir une incidence financière importante. Dans de telles situations, un processus supplémentaire d'analyse coûts-avantages ou coût-efficacité pour appuyer l'évaluation des risques de sécurité peut se justifier. Ceci garantira que l'analyse coût-efficacité ou la justification de mesures recommandées de maîtrise des risques de sécurité a été prise en considération, avec les incidences financières qui s'y rattachent.

Chapitre 3

CULTURE DE LA SÉCURITÉ

3.1 INTRODUCTION

3.1.1 Une culture de la sécurité est la conséquence naturelle de la présence d'humains dans le système d'aviation. La culture de la sécurité a été décrite comme « la façon dont les humains se comportent vis-à-vis de la sécurité et du risque lorsque personne ne les observe ». Elle traduit la façon dont la sécurité est perçue, appréciée et priorisée par la direction et par les employés d'une organisation et la mesure dans laquelle les individus et les groupes :

a) sont conscients des risques et des dangers connus auxquels l'organisation et ses activités sont confrontées ;

b) ont en tout temps un comportement visant à préserver et à renforcer la sécurité ;

c) sont capables d'accéder aux ressources requises pour assurer la sécurité de l'exploitation ;

d) sont désireux et capables de s'adapter lorsqu'ils sont confrontés à des problèmes de sécurité ;

e) sont disposés à communiquer des problèmes de sécurité ;

f) évaluent en permanence les comportements en matière de sécurité dans l'ensemble de l'organisation.

3.1.2 L'Annexe 19 exige que tant les États que les prestataires de services encouragent une culture positive de la sécurité afin de favoriser la mise en œuvre efficace de la gestion de la sécurité au moyen des PNS/SGS. Ce chapitre donne des indications sur la promotion d'une culture positive de la sécurité.

3.2 CULTURE DE LA SÉCURITÉ ET GESTION DE LA SÉCURITÉ

3.2.1 Qu'une organisation en soit consciente ou non, elle aura plusieurs « cultures de la sécurité » différentes, qui reflètent les attitudes et comportements au niveau des groupes. Il n'y a pas deux organisations identiques et même au sein de la même organisation, des groupes différents peuvent avoir des manières diverses d'envisager la sécurité, de parler de la sécurité et de résoudre les problèmes de sécurité. Cette variation peut être appropriée pour des activités différentes.

3.2.2 La façon dont la direction et le personnel intègrent les valeurs de sécurité dans leurs pratiques affecte directement la mise en place et le maintien d'éléments clés du PNS et du SGS. En conséquence, la culture de la sécurité a une incidence directe sur la performance de sécurité. Ne pas accorder une grande importance à la sécurité, c'est risquer des contournements des règles, des raccourcis ou une prise de décisions dangereuses ou de jugements dangereux, surtout lorsque le risque est perçu comme faible et qu'il n'y a pas de conséquence ou de danger manifeste. La culture de la sécurité d'une organisation influence donc considérablement l'élaboration et l'efficacité du PNS ou du SGS. On peut affirmer que la culture de la sécurité est l'élément qui pèse le plus sur la gestion de la sécurité. Si une organisation a adopté toutes les exigences en matière de gestion de la sécurité mais n'a pas une culture positive de la sécurité, elle risque une mauvaise performance.

3.2.3 Lorsqu'une organisation a une culture positive de la sécurité, visiblement soutenue par la haute direction et par les cadres moyens, le personnel en première ligne tend à avoir un sens de la responsabilité partagée dans la réalisation des objectifs de sécurité de l'organisation. Une gestion efficace de la sécurité appuie en outre les efforts tendant à pousser l'organisation vers une culture de la sécurité de plus en plus positive, en rendant le soutien de la direction toujours plus visible et en améliorant la participation active du personnel à la gestion des risques de sécurité.

3.2.4 Une culture positive de la sécurité repose sur un degré élevé de confiance et de respect entre le personnel et la direction. Il faut du temps et des efforts pour développer une culture positive de la sécurité, qui peut facilement pâtir de décisions et d'actions, voire d'inactions, de la direction. Il faut un effort et un renforcement permanents. Lorsque les dirigeants soutiennent activement les pratiques sûres, celles-ci deviennent le mode de fonctionnement normal. La situation idéale est un PNS/SGS pleinement mis en œuvre et efficace et une culture positive de la sécurité. La culture de la sécurité d'une organisation est dès lors souvent perçue comme un reflet de la maturité de son PNS/SGS. Une gestion efficace de la sécurité crée les conditions de développement d'une culture positive de la sécurité et celle-ci crée, à son tour, les conditions pour une gestion efficace de la sécurité.

3.2.5 La culture de la sécurité et son influence sur les comptes rendus de sécurité

3.2.5.1 Les PNS et SGS sont soutenus par les données de sécurité et les informations de sécurité qui sont nécessaires pour traiter les carences et dangers existants et potentiels en matière de sécurité, notamment les problèmes de sécurité constatés par le personnel. Le succès d'un système de compte rendu dépend entièrement du flux continu d'informations provenant des organisations et des individus et des retours d'informations vers ceux-ci. La protection des données de sécurité, des informations de sécurité et des sources connexes est essentielle pour garantir la disponibilité permanente d'informations. Par exemple, dans des systèmes de compte rendu volontaire en matière de sécurité, cette protection peut être réalisée par le biais d'un système confidentiel et non utilisé à d'autres fins que le maintien ou l'amélioration de la sécurité. Les avantages sont doubles. Souvent le personnel est le plus proche des dangers pour la sécurité ; un système de compte rendu volontaire lui permet donc d'identifier activement ces dangers et de suggérer des solutions réalistes. Parallèlement, l'autorité de réglementation ou la direction est à même de recueillir des informations de sécurité importantes et de développer la confiance avec les organisations ou avec le personnel d'exploitation qui communique ces informations. Pour plus d'informations sur la protection des données de sécurité et des informations de sécurité, voir le Chapitre 7.

3.2.5.2 La disposition des organisations ou des individus à rendre compte de leurs expériences et de leurs erreurs dépend en grande partie de leur perception des avantages et inconvénients liés à de tels comptes rendus. Les comptes rendus en matière de sécurité peuvent être anonymes ou confidentiels. En général, dans un système de compte rendu anonyme, l'auteur ne mentionne pas son identité. Dans ce cas, il est impossible d'obtenir des clarifications sur le contenu du compte rendu ou de donner des retours d'informations. Dans un système de compte rendu confidentiel, tout renseignement identifiant l'auteur est connu uniquement d'un dépositaire désigné. Si des organisations et des individus rendant compte de problèmes de sécurité sont protégés et traités de façon juste et cohérente, ils sont plus susceptibles de divulguer de telles informations et de collaborer avec l'autorité de réglementation ou la direction pour gérer efficacement le ou les risques de sécurité qui y sont associés.

3.2.5.3 Les États doivent adopter des lois pour respecter les dispositions de l'Annexe 19 visant à protéger les données de sécurité, les informations de sécurité et les sources connexes. Dans le cas d'un système de compte rendu volontaire, la confidentialité devrait être garantie et le système de compte rendu devrait fonctionner conformément aux lois sur la protection de la sécurité. De plus, des organisations doivent avoir une politique disciplinaire appropriée, accessible à tous et comprise par tous. Une politique disciplinaire devrait indiquer clairement les comportements considérés comme inacceptables et la façon dont l'organisation réagira à de tels comportements. La politique disciplinaire doit être appliquée de façon juste, raisonnable et cohérente. Enfin, les organisations et les individus sont plus susceptibles de rendre compte de leurs expériences et de leurs erreurs dans un environnement dans lequel ils ne seront pas jugés ou traités de manière injuste par leurs pairs ou par leur employeur.

3.2.5.4 D'un point de vue général, les organisations et les individus doivent être convaincus qu'ils seront soutenus lorsqu'ils rendront compte de problèmes dans l'intérêt de la sécurité. Ces comptes rendus incluent les erreurs et les fautes des organisations et des individus. Une augmentation des comptes rendus confidentiels et une baisse des comptes rendus anonymes constituent généralement un signe que l'organisation progresse vers une culture positive de la sécurité.

3.2.6 Culture de la sécurité et diversité culturelle

3.2.6.1 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 obligations de rendre compte, la moralité, les objectifs et les différents régimes juridiques.

3.2.6.2 Dans une perspective de gestion de la sécurité, la culture nationale influence la culture organisationnelle et contribue largement à déterminer la nature et la portée des politiques d'application des règlements, y compris les relations entre le personnel de l'autorité de réglementation et le personnel de l'industrie, et la mesure dans laquelle les informations de sécurité sont protégées. Ces aspects influent à leur tour sur la disposition des personnes à rendre compte de problèmes de sécurité.

3.2.6.3 Actuellement, la majorité des organisations emploient du personnel ayant des origines culturelles très diverses, pouvant être définies par leur nationalité, leur appartenance ethnique, leur religion et/ou leur genre. Les opérations et la sécurité de l'aviation s'appuient sur une interaction efficace entre divers groupes professionnels, qui ont chacun leur propre culture professionnelle. En conséquence, la culture de la sécurité d'une organisation peut aussi être considérablement affectée par la diversité des origines culturelles des membres du personnel.

3.2.6.4 La gestion de la sécurité au sein du système d'aviation exige dès lors une interaction avec du personnel culturellement hétérogène et la gestion de ce personnel hétérogène. Toutefois, lorsqu'ils mettent en œuvre une gestion de la sécurité, les dirigeants devraient être capables de constituer des équipes efficaces avec leur main-d'œuvre hétérogène sur le plan culturel. Pour y parvenir, il est essentiel qu'ils éliminent les différences de perception des risques de sécurité pouvant découler de différentes interprétations culturelles et qu'ils renforcent d'autres aspects liés à la sécurité, tels que la communication, les styles de leadership et l'interaction entre superviseurs et subordonnés. Le succès dépendra de la capacité de la direction à promouvoir une compréhension commune de la sécurité et le rôle de chacun dans l'efficacité de la sécurité. Indépendamment de l'origine culturelle des individus, une gestion efficace de la sécurité repose sur une culture partagée de la sécurité, dans laquelle chaque membre de l'organisation comprend comment il est censé se comporter au regard de la sécurité et du risque « même lorsque personne ne l'observe ».

3.2.7 Culture de la sécurité et changement organisationnel

La gestion de la sécurité exige que les organisations gèrent les risques de sécurité associés aux changements organisationnels et opérationnels. Des changements importants au sein de l'organisation génèrent des préoccupations du personnel au sujet de la charge de travail, de la sécurité de l'emploi et de l'accès à la formation et peuvent avoir une incidence négative sur la culture de la sécurité. La mesure dans laquelle le personnel se sent associé à l'élaboration du changement et comprend son rôle dans ce processus aura aussi une influence sur la culture de la sécurité.

3.3 DÉVELOPPER UNE CULTURE POSITIVE DE LA SÉCURITÉ

3.3.1 Une culture positive de la sécurité est révélée par les caractéristiques suivantes :

a) la direction et les employés veulent, individuellement et collectivement, prendre des décisions et des mesures qui favorisent la sécurité ;

b) les individus et les groupes jettent continuellement un regard critique sur leurs comportements et processus et accueillent favorablement les critiques des autres, dans une volonté de rechercher des occasions de changer et de s'améliorer à mesure que leur environnement évolue ;

c) la direction et le personnel partagent une conscience commune des dangers et risques auxquels sont confrontées l'organisation et ses activités, et de la nécessité de gérer les risques ;

d) les individus agissent et prennent des décisions en fonction d'une conviction commune que la sécurité fait partie intégrante de la conduite des affaires ;

e) les individus apprécient d'être informés, et d'informer d'autres, sur la sécurité ;

f) les individus confient à leurs collègues et à leurs directeurs des informations sur leurs expériences et les comptes rendus d'erreurs et de fautes sont encouragés afin d'améliorer les façons de procéder à l'avenir.

3.3.2 Les actions de la direction et des employés peuvent contribuer à rendre leur culture de la sécurité plus positive. Le Tableau 5 donne des exemples des types d'actions de la direction et des employés qui faciliteront ou entraveront une culture positive de la sécurité au sein d'une organisation. Les organisations devraient s'attacher à mettre en place les éléments facilitateurs et à éliminer les entraves pour promouvoir et atteindre une culture positive de la sécurité.

Tableau 5. Exemples d'actions qui faciliteront ou entraveront une culture positive de la sécurité

Élément	*Description générale*	*Éléments facilitateurs*	*Entraves*
Engagement envers la sécurité			
L'engagement envers la sécurité reflète la mesure dans laquelle la haute direction de l'organisation a une attitude positive envers la sécurité et reconnaît son importance. La haute direction devrait être véritablement déterminée à atteindre et à maintenir un niveau élevé de sécurité et devrait donner aux employés la motivation et les moyens d'y parvenir.		• La direction montre la voie en matière de culture de la sécurité et motive activement ses employés à se soucier de la sécurité, pas seulement en paroles mais en montrant l'exemple. • La direction fournit les ressources pour une gamme de tâches liées à la sécurité (p. ex. la formation). • Une supervision et une gouvernance continues de la gestion de la sécurité sont mises en place.	• La direction montre activement qu'elle donne la priorité au profit, à la réduction des coûts et à l'efficacité. • Les investissements pour améliorer la sécurité sont souvent faits lorsque les règlements l'exigent ou après des accidents. • Ni une supervision ni une gouvernance ne sont mises en place pour la gestion de la sécurité.

Élément	*Description générale*	*Éléments facilitateurs*	*Entraves*
Adaptabilité			
L'adaptabilité reflète la mesure dans laquelle les employés et la direction sont disposés à tirer des leçons des expériences passées et sont capables de prendre les mesures nécessaires pour renforcer le niveau de sécurité au sein de l'organisation.		• Les contributions des employés sont activement encouragées lorsqu'il s'agit de résoudre des problèmes de sécurité. • Tous les incidents et les constatations d'audits sont analysés et des mesures sont prises en conséquence. • L'incidence des processus et procédures organisationnels sur la sécurité est analysée (degré élevé d'autocritique). • Une approche proactive claire de la sécurité est mise en évidence et suivie.	• Le personnel de tous les échelons n'est pas invité à livrer ses idées sur les questions de sécurité. • Des mesures sont souvent prises uniquement après des accidents ou lorsque les réglementations l'exigent. • Les processus et procédures organisationnels sont considérés comme adéquats tant qu'il ne se produit pas d'accidents (excès de confiance ou manque d'autocritique). • Même lorsqu'un accident se produit, l'organisation n'est pas disposée à se remettre en question. • Une approche réactive de la sécurité est mise en évidence et suivie.
Sensibilisation			
La sensibilisation reflète la mesure dans laquelle les employés et la direction sont conscients des risques pour l'aviation auxquels l'organisation et ses activités sont confrontées. Du point de vue de l'État, le personnel est conscient des risques de sécurité induits à la fois par ses propres activités et par les organisations qu'il supervise. Les employés et la direction devraient maintenir à tout moment un degré élevé de vigilance à l'égard des problèmes de sécurité.		• Un mode efficace d'identification des dangers a été mis en place. • Des enquêtes cherchent à déterminer la cause première. • L'organisation se tient au courant d'importantes améliorations de la sécurité et s'adapte en conséquence, si nécessaire.	• Aucun effort n'est consenti pour identifier les dangers. • Les enquêtes s'arrêtent dès la détermination de la première cause plausible, sans chercher la cause première. • L'organisation ne se tient pas au courant d'importantes améliorations de la sécurité.

Élément	*Description générale*	*Éléments facilitateurs*	*Entraves*
		• L'organisation évalue systématiquement si les améliorations de la sécurité sont mises en œuvre et fonctionnent comme prévu. • Les membres appropriés de l'organisation sont bien conscients des risques de sécurité induits par leurs actions individuelles et par les opérations/activités de la compagnie.	• L'organisation n'évalue pas systématiquement si les améliorations de la sécurité sont mises en œuvre de façon appropriée. • Les membres appropriés de l'organisation ne sont pas conscients des risques de sécurité induits par leurs actions individuelles et par les opérations de la compagnie. • Des données de sécurité sont recueillies mais pas analysées et aucune mesure n'est prise en conséquence.
Comportement vis-à-vis de la sécurité			
Le comportement vis-à-vis de la sécurité reflète la mesure dans laquelle chaque niveau de l'organisation se comporte de façon à maintenir et à améliorer le niveau de sécurité. L'importance de la sécurité devrait être reconnue et les processus et procédures requis pour maintenir la sécurité devraient être en place.		• Les employés se motivent à agir en toute sécurité et à montrer l'exemple. • Un suivi continu des comportements sûrs est pratiqué. • Des comportements dangereux intentionnels ne sont pas tolérés par la direction ni par les collègues. • Les conditions de travail favorisent la sécurité de l'aviation à tout moment.	• Les employés ne sont pas punis pour des comportements dangereux intentionnels appliqués dans leur intérêt ou dans celui d'un autre. • Les conditions de travail induisent des comportements et des contournements des règles néfastes pour la sécurité de l'aviation. • Aucun suivi de la sécurité de l'aviation n'est pratiqué concernant les produits ou services de l'organisation. • Des critiques constructives au bénéfice de la sécurité de l'aviation ne sont pas accueillies favorablement.

Élément	*Description générale*	*Éléments facilitateurs*	*Entraves*
Information			
Cet élément reflète la mesure dans laquelle l'information est diffusée à toutes les personnes nécessaires au sein de l'organisation. Les employés devraient être habilités et encouragés à rendre compte de préoccupations relatives à la sécurité de l'aviation et devraient recevoir des retours d'informations sur leurs comptes rendus. Les informations de travail relatives à la sécurité de l'aviation doivent être communiquées judicieusement aux bonnes personnes afin d'éviter de mauvaises communications susceptibles de générer des situations et des conséquences dangereuses pour le système d'aviation. L'État est prêt à partager les informations liées à la sécurité de l'aviation avec tous les prestataires de services.		• Il existe un environnement ouvert et juste de compte rendu de sécurité. • Les employés reçoivent en temps utile des informations pertinentes pour la sécurité afin qu'ils puissent assurer la sécurité de l'exploitation ou prendre des décisions sûres. • La direction et les superviseurs vérifient régulièrement si les informations pertinentes pour la sécurité sont comprises et si des mesures sont prises en conséquence. • Des transferts de connaissances et des formations sur la sécurité de l'aviation sont effectués (p. ex. partage des leçons tirées).	• Un environnement accusateur manifeste accueille les comptes rendus de sécurité. • Il y a rétention des informations pertinentes pour la sécurité. • L'efficacité de la communication en matière de sécurité n'est pas surveillée. • Aucun transfert de connaissances ou aucune formation n'est fourni.
Confiance			
La contribution des employés à la sécurité est stimulée dans un environnement de compte rendu qui favorise la confiance — confiance que les actions ou omissions des travailleurs, proportionnelles à leur formation et à leur expérience, ne seront pas punies. Une approche réaliste consiste à pratiquer une évaluation du caractère raisonnable, c'est-à-dire à déterminer si une personne du même niveau d'expérience et de formation pourrait faire la même chose. Un tel environnement est indispensable pour des comptes rendus de sécurité efficaces et efficients.		• Une distinction est établie entre les comportements acceptables et inacceptables, distinction connue de tous les employés. • Les enquêtes sur les événements (y compris les accidents et incidents) examinent les facteurs individuels et organisationnels.	• Aucune distinction n'est établie entre les comportements acceptables et inacceptables. • Les employés sont systématiquement et sévèrement punis pour des erreurs humaines.

Élément	*Description générale*	*Éléments facilitateurs*	*Entraves*
Des systèmes efficaces de compte rendu de sécurité contribuent à garantir que les personnes sont disposées à rendre compte de leurs erreurs et expériences afin que les États et les prestataires de services aient accès aux données et informations pertinentes qui sont nécessaires pour s'attaquer aux carences et aux dangers de sécurité existants et potentiels. Ces systèmes créent un environnement dans lequel les personnes peuvent avoir la certitude que les données de sécurité et les informations de sécurité seront utilisées exclusivement pour améliorer la sécurité.		• Une bonne performance de sécurité de l'aviation est reconnue et récompensée de façon régulière. • Les employés et le personnel d'exploitation sont disposés à rendre compte d'événements auxquels ils ont été associés.	• Les enquêtes sur les accidents et sur les événements se concentrent uniquement sur les facteurs individuels. • Une bonne performance de sécurité et des comportements sûrs sont considérés comme naturels.

3.3.3 Suivi de la culture de la sécurité

3.3.3.1 La culture de la sécurité subit de nombreuses influences et les organisations peuvent choisir d'évaluer leur culture de la sécurité pour :

a) comprendre la perception que les gens ont de l'organisation et le degré d'importance accordé à la sécurité ;

b) identifier les points forts et les points faibles ;

c) identifier les différences entre divers groupes (sous-cultures) au sein d'une organisation ;

d) examiner les évolutions au fil du temps (p. ex. en réponse à des changements organisationnels importants tels que ceux qui sont introduits après un accident, un changement de la haute direction ou des modifications des arrangements régissant les relations sociales).

3.3.3.2 Plusieurs outils sont utilisés, souvent en combinaison, pour évaluer la maturité de la culture de la sécurité :

a) questionnaires ;

b) entretiens et groupes de travail ;

c) observations ;

d) examens de documents.

3.3.3.3 L'évaluation de la maturité de la culture de la sécurité peut fournir des indications précieuses qui permettront à la direction de prendre des mesures afin d'encourager les comportements souhaités en matière de sécurité. Il convient de noter que ces évaluations sont sujettes à une certaine subjectivité et peuvent refléter les points de vue et perceptions des personnes concernées à un moment spécifique seulement. De plus, une notation de la maturité de la culture de la sécurité peut avoir des conséquences non souhaitées, notamment en encourageant involontairement l'organisation à s'efforcer d'atteindre la « bonne » note plutôt qu'à amener ses membres à travailler ensemble pour comprendre et améliorer la culture de la sécurité.

———————

Chapitre 4

GESTION DE LA PERFORMANCE DE SÉCURITÉ

4.1 INTRODUCTION

4.1.1 La gestion de la performance de sécurité est au cœur du fonctionnement du PNS et des SGS. Bien mise en œuvre, elle donne à une organisation les moyens de déterminer si ses activités et processus sont efficaces pour atteindre ses objectifs en matière de sécurité. Pour ce faire, il faut identifier les indicateurs de performance de sécurité (SPI) utilisés pour le suivi et la mesure de la performance de sécurité. L'identification des SPI permet d'obtenir des informations qui permettront à la haute direction de prendre conscience de la situation actuelle et de soutenir le processus décisionnel, notamment en déterminant si des mesures sont requises pour atténuer davantage les risques de sécurité afin de garantir que l'organisation atteigne ses objectifs de sécurité.

4.1.2 La Figure 4-1 ci-dessous présente le processus générique de gestion de la performance de sécurité et sa corrélation avec les systèmes de collecte et de traitement des données de sécurité (SDCPS) et avec l'analyse de sécurité, qui sont examinés aux Chapitres 5 et 6, respectivement. Le lien avec la promotion de la sécurité est mis en évidence pour souligner combien il est important de communiquer ces informations dans l'ensemble de l'organisation. De plus amples informations sur la promotion de la sécurité, un élément important du PNS et des SGS qui est souvent sous-estimé, figurent aux Chapitres 8 et 9, respectivement.

4.1.3 La gestion de la performance de sécurité aide l'organisation à poser les quatre questions les plus importantes en matière de gestion de la sécurité et à y répondre :

a) Quels sont les principaux risques de sécurité de l'organisation ? *Déduits d'une analyse des données sur les accidents et les incidents d'aviation ainsi que d'une analyse prédictive visant à identifier et à définir les risques émergents.*

b) Quels objectifs de sécurité l'organisation s'est-elle fixés et quels sont les principaux risques de sécurité à traiter ? *Les objectifs de sécurité de l'organisation.*

c) Comment l'organisation saura-t-elle si elle progresse vers la réalisation de ses objectifs de sécurité ? *Par le biais des SPI, des SPT et, le cas échéant, des facteurs déclencheurs en matière de sécurité.*

d) Quelles données de sécurité et quelles informations de sécurité sont requises pour prendre des décisions en matière de sécurité en connaissance de cause ? Y compris l'affectation des ressources de l'organisation. *Par le biais d'un SDCPS évolutif et d'une analyse des données de sécurité.*

4.1.4 Le processus de gestion de la performance de sécurité peut aussi être utilisé pour établir un niveau acceptable de performance de sécurité (ALoSP). Le Chapitre 8 contient de plus amples indications sur l'établissement d'un ALoSP.

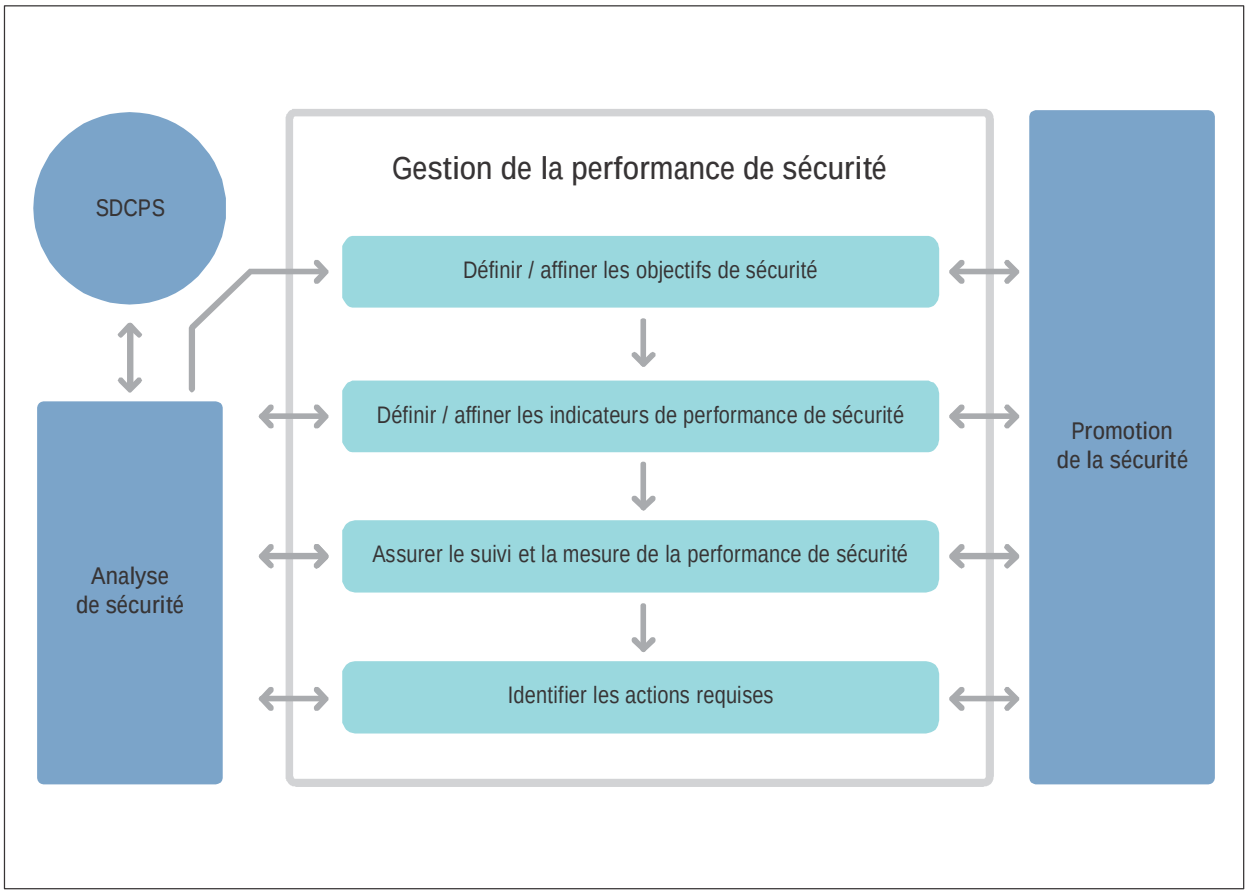

Figure 4-1. Processus de gestion de la performance de sécurité

4.1.5 Relation entre les États et les prestataires de services

4.1.5.1 Il existe des similitudes entre l'État et les prestataires de services en ce qui concerne l'utilisation et l'application des techniques de performance de sécurité. Les orientations présentées dans ce chapitre ont été élaborées tant pour les États que pour les prestataires de services mais certaines différences sont mises en évidence dans cette section.

4.1.5.2 La détermination de la performance de sécurité d'un État devrait se concentrer sur ce que cet État considère comme les aspects les plus importants pour gérer la sécurité. L'État utilise un PNS mis en œuvre avec efficacité comme outil de prise de décisions pour la gestion de la performance de sécurité, gestion qui devrait inclure la performance de sécurité des prestataires de services dans cet État, la capacité de supervision de cet État, et l'appui fourni aux prestataires de services par l'établissement de lignes directrices. Les États devraient envisager de mesurer leur capacité à :

a) maintenir leur système de supervision de la sécurité ;

b) appliquer des mesures de sécurité spécifiques et introduire des initiatives en matière de sécurité ;

c) adapter les mesures en vigueur pour la maîtrise des risques de sécurité afin de garantir que ces mesures restent efficaces.

4.1.5.3 Pour les prestataires de services, la fonction première de la gestion de la performance de sécurité est de surveiller et mesurer leur efficacité à gérer leurs risques de sécurité. Cela requiert une mise en œuvre efficace d'un SGS qui génère des informations qui seront utilisées pour prendre des décisions en matière de gestion de la sécurité, y compris la mise en place de mesures de maîtrise des risques de sécurité et l'affectation de ressources.

4.1.5.4 La réussite de la gestion de la sécurité dépend de l'engagement entre l'État et ses prestataires de services. Il peut être avantageux que l'État identifie des SPI appropriés pouvant être suivis par les prestataires de services et ensuite partagés avec l'État, en particulier pour l'établissement de l'ALoSP (voir Chapitre 8 pour plus d'informations). Les informations reçues des prestataires de services aideront l'État dans son évaluation de la performance de sécurité de son industrie aéronautique et de sa propre capacité à assurer une supervision et un appui efficaces aux prestataires de services. Toutefois, les prestataires de services devraient s'assurer que leurs SPI sont bien appropriés à leur contexte opérationnel, à leur historique de performance et à leurs attentes.

4.1.6 Gestion de la performance de sécurité et interfaces

4.1.6.1 Lorsque les États et les prestataires de services envisagent de mettre en œuvre une gestion de la sécurité, il est important qu'ils prennent en considération les risques de sécurité induits par les interfaces entre les entités. Les interfaces peuvent être internes (p. ex. entre l'exploitation et la maintenance ou entre les services des finances, des ressources humaines ou le service juridique) ou elles peuvent être externes (p. ex. un autre État, des prestataires de services ou des sous-traitants). Les dangers et les risques connexes aux points d'interface comptent parmi les facteurs les plus courants contribuant à des événements de sécurité. Les États et les prestataires de services ont une meilleure maîtrise des risques de sécurité liés aux interfaces lorsque leurs interfaces sont identifiées et gérées. Les interfaces devraient être définies dans la description du système de l'organisation.

4.1.6.2 Les États et les prestataires de services sont responsables du suivi et de la gestion en continu de leurs interfaces afin de garantir des résultats sûrs. Le risque de sécurité présenté par chaque interface devrait, idéalement, être évalué de façon collaborative par les entités en interface. Une collaboration est hautement souhaitable parce que la perception des risques de sécurité et de leur tolérabilité peut varier entre les organisations en interface. Le partage de la gestion des risques aux interfaces, par la mise en place et le suivi de SPI, encourage la sensibilisation mutuelle aux risques de sécurité plutôt que l'ignorance ou une gestion des risques potentiellement unilatérale. Il offre en outre une occasion de transfert de connaissances et de pratiques de travail pouvant améliorer l'efficacité de la sécurité des deux organisations.

4.1.6.3 C'est pourquoi il convient de convenir de SPI et de mettre ceux-ci en place pour suivre et mesurer les risques et l'efficacité des mesures d'atténuation. Un accord formel de gestion des interfaces entre les organisations en interface, avec des responsabilités de suivi et de gestion clairement définies, constitue un exemple d'approche efficace.

4.2. OBJECTIFS DE SÉCURITÉ

4.2.1 Les objectifs de sécurité sont de brèves déclarations de haut niveau sur les réalisations en matière de sécurité ou sur le résultat escompté à atteindre. Les objectifs de sécurité donnent une direction aux activités de l'organisation et devraient donc être cohérents avec la politique de sécurité, qui énonce l'engagement de haut niveau de l'organisation à garantir la sécurité. Ils sont aussi utiles pour communiquer les priorités en matière de sécurité au personnel et à l'ensemble de la communauté aéronautique. L'établissement d'objectifs de sécurité donne une direction stratégique au processus de gestion de la performance de sécurité et fournit une base solide pour la prise de décisions en matière de sécurité. La gestion de la performance de sécurité devrait être un élément fondamental à prendre en considération lors de la modification de politiques ou de processus ou lors de l'affectation des ressources de l'organisation en vue d'améliorer la performance de sécurité.

4.2.2 Les objectifs de sécurité peuvent être :

a) *axés sur les processus :* formulés en termes de comportements sûrs attendus du personnel d'exploitation ou de l'exécution d'actions mises en œuvre par l'organisation pour gérer les risques de sécurité ;

b) *axés sur les résultats :* englobant les actions et tendances en matière de limitation des accidents ou des pertes opérationnelles.

4.2.3 L'ensemble des objectifs de sécurité devrait inclure une combinaison d'objectifs axés sur les processus et d'objectifs axés sur les résultats pour assurer une couverture et une direction suffisantes pour les SPI et les SPT. Si les objectifs de sécurité et les SPI et SPT qui y sont associés forment un ensemble qui permet à une organisation de prouver qu'elle maintient ou améliore sa performance de sécurité, il n'est pas nécessaire que les objectifs de sécurité soient, en eux-mêmes, spécifiques, mesurables, réalisables, pertinents et opportuns (SMART) (George T. Doran, 1981).

Tableau 6. Exemples d'objectifs de sécurité

Exemples d'objectifs de sécurité		
Axés sur les processus	État ou prestataire de services	Accroître les niveaux de compte rendu de sécurité.
Axés sur les résultats	Prestataire de services	Réduire le taux d'événements de sécurité indésirables sur les aires de trafic. (haut niveau) ou Réduire le nombre annuel d'événements de sécurité indésirables sur les aires de trafic par rapport à l'année précédente.
Axés sur les résultats	État	Réduire le nombre annuel d'événements de sécurité dans le secteur X.

4.2.4 Une organisation peut aussi choisir d'identifier des objectifs de sécurité au niveau tactique ou opérationnel et de les appliquer à des projets, produits et processus spécifiques. Un objectif de sécurité peut aussi être exprimé par l'utilisation d'autres termes ayant une acception similaire (p. ex. but ou cible).

4.3 INDICATEURS DE PERFORMANCE DE SÉCURITÉ ET CIBLES DE PERFORMANCE DE SÉCURITÉ

4.3.1 Types d'indicateurs de performance de sécurité

Indicateurs qualitatifs et quantitatifs

4.3.1.1 Les SPI sont utilisés pour aider la haute direction à savoir si l'organisation est susceptible d'atteindre son objectif de sécurité ; ils peuvent être qualitatifs ou quantitatifs. Les indicateurs quantitatifs visent à mesurer par la quantité, plutôt que par la qualité, tandis que les indicateurs qualitatifs sont descriptifs et mesurent en fonction de la qualité. Les indicateurs quantitatifs sont préférés aux indicateurs qualitatifs parce qu'ils sont plus faciles à chiffrer et à

comparer. Le choix de l'indicateur dépend de la disponibilité de données fiables pouvant être mesurées de façon quantitative. Les preuves nécessaires doivent-elles être sous la forme de données (quantitatives) comparables, généralisables ou sous la forme d'une image descriptive de la situation en matière de sécurité (qualitative) ? Chacune de ces options (qualitative ou quantitative) induit des types différents de SPI et exige un processus de sélection des SPI mûrement réfléchi. Une combinaison d'approches est utile dans de nombreuses situations et peut résoudre nombre des problèmes pouvant se poser lorsqu'on adopte une approche unique. Un exemple d'indicateur qualitatif pourrait être, pour un État, la maturité du SGS de ses prestataires de services dans un secteur particulier ou, pour un prestataire de services, l'évaluation de la culture de la sécurité.

4.3.1.2 Les indicateurs quantitatifs peuvent être exprimés par un chiffre (x incursions) ou par un taux (x incursions par n mouvements). Dans certains cas, une expression numérique sera suffisante. Toutefois, la seule utilisation de chiffres peut créer une impression déformée de la situation réelle de la sécurité si le niveau d'activité fluctue. Par exemple, si le contrôle de la circulation aérienne enregistre trois écarts soudains d'altitude en juillet et six en août, on pourrait gravement s'inquiéter de la détérioration significative de la performance de sécurité. Mais il peut y avoir eu deux fois plus de mouvements en août qu'en juillet, ce qui signifie que le nombre d'écarts soudains d'altitude par mouvement, soit le taux, a diminué et non augmenté. Cela peut modifier ou non le niveau d'attention accordé mais fournit néanmoins un nouvel élément précieux d'information susceptible d'être crucial pour une prise de décisions fondée sur les données en matière de sécurité.

4.3.1.3 C'est pourquoi, le cas échéant, les SPI devraient être exprimés en fonction d'un taux relatif pour mesurer le niveau de performance indépendamment du niveau d'activité. Un tel taux relatif offre une mesure normalisée de la performance, que l'activité augmente ou diminue. Un autre exemple serait qu'un SPI mesure le nombre d'incursions sur piste. Mais s'il y a eu moins de départs dans la période visée, le résultat pourrait être trompeur. Une mesure plus précise et plus utile de la performance serait le nombre d'incursions sur piste par rapport au nombre de mouvements, par exemple x incursions par 1 000 mouvements.

Indicateurs retardés et avancés

4.3.1.4 Les deux catégories les plus courantes utilisées par les États et les prestataires de services pour classer leurs SPI sont les indicateurs retardés et avancés. Les SPI retardés mesurent les événements qui se sont déjà produits. Ils sont aussi appelés « SPI fondés sur les résultats » et traduisent normalement (mais pas toujours) les résultats négatifs que l'organisation vise à éviter. Les SPI avancés mesurent les processus et intrants mis en œuvre pour améliorer ou maintenir la sécurité. Ils sont aussi appelés « SPI fondés sur les activités ou les processus » car ils surveillent et mesurent les conditions pouvant mener ou contribuer à un résultat spécifique.

4.3.1.5 Les SPI retardés aident l'organisation à comprendre ce qui s'est produit par le passé et sont utiles pour l'établissement de tendances à long terme. Ils peuvent être utilisés en tant qu'indicateurs de haut niveau ou comme indications de types ou de lieux spécifiques d'événements, tels que les « types d'accidents par type d'aéronef » ou les « types d'incidents spécifiques par région ». Comme les SPI retardés mesurent les résultats en matière de sécurité, ils peuvent mesurer l'efficacité des mesures d'atténuation des risques de sécurité. Ils sont efficaces pour valider la performance de sécurité générale du système. Par exemple, le suivi du « nombre de collisions sur aires de trafic par nombre de mouvements entre véhicules après une modification des marquages des aires de trafic » fournit une mesure de l'efficacité des nouveaux marquages (en supposant qu'aucun autre paramètre n'ait changé). La réduction des collisions valide une amélioration de la performance de sécurité générale du système des aires de trafic, qui peut être attribuable au changement en question.

4.3.1.6 Les tendances des SPI retardés peuvent être analysées pour déterminer les conditions présentes dans le système auxquelles il convient de remédier. Si nous reprenons l'exemple précédent, une tendance à la hausse des collisions sur aires de trafic par nombre de mouvements peut avoir permis de constater des carences dans le marquage des aires de trafic et de prendre des mesures d'atténuation adéquates.

4.3.1.7 Les SPI retardés se répartissent en deux types :

a) *faible probabilité/forte gravité :* résultats tels qu'accidents ou incidents graves. Vu la faible fréquence de résultats de grande gravité, l'agrégation de données (au niveau du segment de l'industrie ou au niveau régional) peut permettre des analyses plus intéressantes. Un exemple de ce type de SPI retardé serait les « dommages aux aéronefs et/ou aux moteurs dus à des impacts d'oiseaux » ;

b) *forte probabilité/faible gravité :* les résultats ne se sont pas nécessairement manifestés par un accident ou un incident grave ; on parle parfois aussi d'indicateurs précurseurs. Les SPI pour des résultats à forte probabilité/faible gravité sont principalement utilisés pour surveiller des problèmes de sécurité spécifiques et pour mesurer l'efficacité des mesures existantes d'atténuation des risques de sécurité. Un exemple de ce type de SPI précurseur serait les « détections d'oiseaux par radar », qui indique le niveau d'activité aviaire plutôt que le nombre d'impacts d'oiseaux réel.

4.3.1.8 Les mesures de sécurité de l'aviation privilégient traditionnellement des SPI qui reflètent des résultats à « faible probabilité/forte gravité ». C'est compréhensible dans la mesure où les accidents et les incidents graves sont des événements très médiatisés et faciles à dénombrer. Toutefois, vu sous l'angle de la gestion de la performance de sécurité, un appui excessif sur les accidents et sur les incidents graves comme base d'un indicateur fiable de la performance de sécurité comporte des désavantages. Par exemple, les accidents et les incidents graves sont peu fréquents (il peut n'y avoir qu'un seul accident par an, voir aucun), ce qui complique la réalisation d'une analyse statistique en vue d'identifier des tendances. Or, cela n'indique pas nécessairement que le système est sûr. Le fait de se fier à ce type de données peut induire un faux sentiment de certitude que la performance de sécurité de l'organisation ou du système est bonne, alors qu'en réalité, un accident est dangereusement proche.

4.3.1.9 Les SPI avancés sont des mesures qui se concentrent sur les processus et les intrants mis en œuvre pour améliorer ou maintenir la sécurité. Ils sont aussi appelés « SPI fondés sur les activités ou les processus » car ils surveillent et mesurent les circonstances pouvant mener ou contribuer à un résultat spécifique.

4.3.1.10 Parmi les exemples de SPI avancés stimulant le développement de capacités organisationnelles à des fins de gestion proactive de la performance de sécurité, citons « le pourcentage des membres du personnel qui ont terminé avec succès la formation à la sécurité à temps » ou « la fréquence des activités d'effarouchement des oiseaux ».

4.3.1.11 Les SPI avancés peuvent aussi informer l'organisation sur la capacité de son exploitation à s'adapter au changement, y compris aux changements dans son environnement d'exploitation. Ils cibleront soit l'anticipation des points faibles et des vulnérabilités résultant du changement ou le suivi de la performance après un changement. Un exemple de SPI destiné au suivi d'un changement dans l'exploitation serait « le pourcentage de sites ayant mis en œuvre la procédure X ».

4.3.1.12 Pour dégager une indication plus précise et utile de la performance de sécurité, les SPI retardés, qui mesurent à la fois les événements à « faible probabilité/forte gravité » et les événements à « forte probabilité/faible gravité », devraient être combinés à des SPI avancés. La Figure 4-2 illustre le concept d'indicateurs avancés et retardés permettant de livrer une image plus complète et réaliste de la performance de sécurité de l'organisation.

4.3.2 Sélection et définition des SPI

4.3.2.1 Les SPI sont les paramètres qui donnent à l'organisation un panorama de sa performance de sécurité, en présentant son bilan en matière de sécurité pour le passé et pour le présent, ainsi que le cap fixé pour l'avenir. Ce panorama constitue une base solide et défendable sur laquelle l'organisation se fonde pour prendre des décisions fondées sur les données en matière de sécurité. Ces décisions, à leur tour, affectent positivement la performance de sécurité de l'organisation. L'identification des SPI devrait donc être réaliste, pertinente et liée aux objectifs de sécurité, indépendamment de leur simplicité ou de leur complexité.

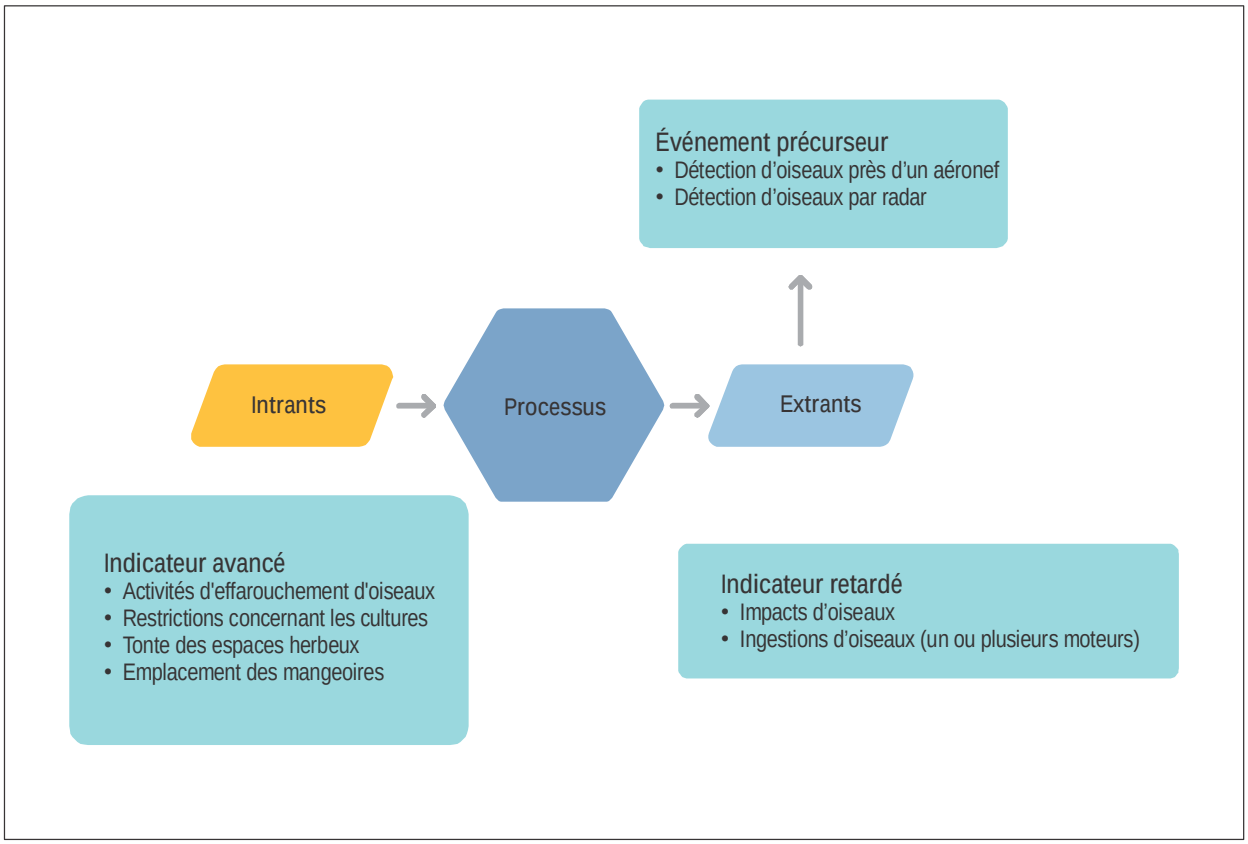

Figure 4-2. Phases conceptuelles des indicateurs avancés ou retardés

4.3.2.2 Il est probable que la sélection initiale de SPI soit limitée au suivi et à la mesure de paramètres représentant des événements ou des processus faciles et/ou commodes à saisir (données de sécurité peut-être déjà disponibles). Idéalement, les SPI devraient se concentrer sur des paramètres qui constituent des indicateurs importants de la performance de sécurité, plutôt que sur ceux qui sont faciles à obtenir.

4.3.2.3 Les SPI devraient être :

a) liés à l'objectif de sécurité qu'ils entendent indiquer ;

b) sélectionnés ou élaborés sur la base de données disponibles et de mesures fiables ;

c) quantifiables et d'une spécificité appropriée ;

d) réalistes, en tenant compte des possibilités et contraintes de l'organisation.

4.3.2.4 Une combinaison de SPI est généralement requise pour livrer une indication claire de la performance de sécurité. Il devrait exister un lien clair entre les SPI retardés et avancés. Idéalement, il faudrait définir les SPI retardés avant de déterminer les SPI avancés. La définition d'un SPI précurseur lié à un événement ou à une circonstance plus grave (le SPI retardé) garantit une corrélation claire entre les deux. Tous les SPI, qu'ils soient retardés ou avancés, sont tout aussi valables et précieux. Un exemple de ces corrélations est illustré à la Figure 4-3.

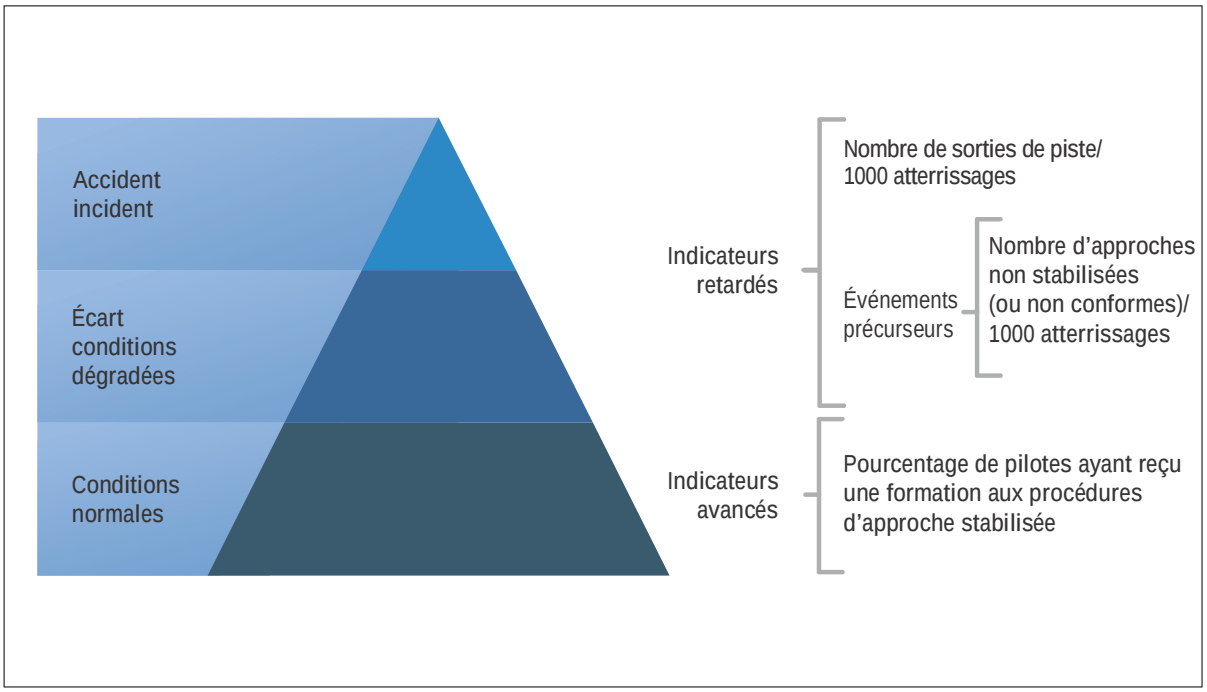

Figure 4-3. Exemples de corrélations entre indicateurs retardés et avancés

4.3.2.5 Il est important de sélectionner des SPI en relation avec les objectifs de sécurité de l'organisation. Des SPI bien définis et alignés facilitent l'identification des SPT, qui montreront les progrès engrangés vers la réalisation des objectifs de sécurité. En sachant précisément ce qui est requis et quand et comment agir pour atteindre la performance de sécurité planifiée, l'organisation pourra affecter des ressources avec un effet maximum sur la sécurité. Par exemple, un État a pour objectif de sécurité de « réduire le nombre de sorties de piste de 50 pour cent en trois ans » et a un SPI associé, bien aligné, mesurant le « nombre de sorties de piste par million de départs dans tous les aérodromes ». Si le nombre de sorties baisse initialement au début du suivi mais commence à augmenter à nouveau après douze mois, l'État pourrait choisir de retirer des ressources d'un domaine où, d'après les SPI, l'objectif de sécurité est facilement atteint pour les affecter à la réduction des sorties de piste afin d'atténuer la tendance non souhaitée.

Définition de SPI

4.3.2.6 Le contenu de chaque SPI devrait inclure :

a) une description de ce que le SPI mesure ;

b) le but du SPI (ce qu'il est censé gérer et qui il est censé informer) ;

c) les unités de mesure et toute exigence pour son calcul ;

d) qui est responsable de la collecte, de la validation, du suivi, du compte rendu et des actions en rapport avec ce SPI (il peut s'agir de membres du personnel de différentes parties de l'organisation) ;

e) où et comment les données devraient être collectées ;

f) la fréquence des comptes rendus, de la collecte, du suivi et de l'analyse des données du SPI.

SPI et comptes rendus en matière de sécurité

4.3.2.7 Tant que l'incidence de changements dans les pratiques d'exploitation n'est pas pleinement acceptée par les déclarants potentiels, il peut y avoir une sous-déclaration des problèmes. C'est ce qu'on appelle « le biais de déclaration ». Des changements dans les dispositions liées à la protection des informations de sécurité et des sources connexes pourraient aussi mener à des surdéclarations. Dans les deux cas, le biais de déclaration peut déformer l'intention et l'exactitude des données utilisées pour le SPI. Employés judicieusement, les comptes rendus en matière de sécurité peuvent toujours fournir des données précieuses pour la gestion de la performance de sécurité.

4.3.3 Fixation des cibles de performance de sécurité

4.3.3.1 Les cibles de performance de sécurité (SPT) définissent les résultats souhaités de la gestion à court et à moyen terme de la performance de sécurité. Elles font office de « jalons » donnant l'assurance que l'organisation est en bonne voie pour réaliser ses objectifs de sécurité et elles fournissent un moyen mesurable de vérifier l'efficacité des activités de gestion de la performance de sécurité. La fixation des SPT devrait tenir compte de facteurs tels que le niveau prédominant de risque de sécurité, la tolérabilité du risque de sécurité ainsi que les attentes en matière de sécurité dans le secteur concerné de l'aviation. La fixation de SPT devrait être déterminée après analyse des objectifs que le secteur de l'aviation concerné peut réalistement atteindre et de la performance récente du SPI spécifique, lorsque des données sur les tendances historiques sont disponibles.

4.3.3.2 Si la combinaison des objectifs de sécurité, des SPI et des SPT est SMART, elle permet à l'organisation de prouver plus efficacement sa performance de sécurité. Il existe de multiples approches pour atteindre les buts de la gestion de la performance de sécurité, en particulier, la fixation de SPT. Une approche consiste à établir des objectifs de sécurité généraux de haut niveau avec des SPI alignés, puis à identifier les niveaux raisonnables d'améliorations après qu'une performance de sécurité de référence a été établie. Ces niveaux d'améliorations peuvent être basés sur des cibles spécifiques (p. ex. baisse de pourcentage) ou sur la réalisation d'une tendance positive. Une autre approche qui peut être utilisée lorsque les objectifs de sécurité sont SMART est de donner aux cibles de sécurité le rôle de jalons pour atteindre les objectifs de sécurité. Ces deux approches sont valables mais les organisations peuvent en estimer d'autres efficaces pour faire la preuve de leur performance de sécurité. Des approches différentes peuvent être utilisées en combinaison selon les circonstances spécifiques.

Fixation de cibles avec des objectifs de sécurité de haut niveau

4.3.3.3 Des cibles sont fixées avec la haute direction, qui convient d'objectifs de sécurité de haut niveau. L'organisation identifie ensuite des SPI appropriés qui montreront l'amélioration de la performance de sécurité vers la réalisation du ou des objectifs de sécurité convenus. Les SPI seront mesurés en utilisant les sources de données existantes mais exigeront peut-être aussi la collecte de données supplémentaires. L'organisation commence alors à collecter, analyser et présenter les SPI. Des tendances commenceront à émerger, ce qui donnera un aperçu de la performance de sécurité de l'organisation et indiquera si celle-ci se rapproche ou s'écarte de ses objectifs de sécurité. À ce stade, l'organisation peut identifier des SPT raisonnables et réalisables pour chaque SPI.

Fixation de cibles avec des objectifs de sécurité SMART

4.3.3.4 Les objectifs de sécurité peuvent être difficiles à communiquer et peuvent sembler difficiles à atteindre ; en les subdivisant en cibles de sécurité concrètes de plus petite ampleur, le processus de réalisation des objectifs sera plus facile à gérer. Ainsi, les cibles constituent un lien crucial entre la stratégie et les opérations quotidiennes. Les organisations devraient identifier des domaines clés faisant progresser la performance de sécurité et établir un moyen de les mesurer. Une fois qu'une organisation connaît son niveau actuel de performance en établissant la performance de sécurité de référence, elle peut commencer à fixer des SPT pour donner à chacun dans l'État une idée claire de ce qu'il faut tenter d'atteindre. L'organisation peut aussi utiliser des études comparatives pour appuyer la fixation des cibles

de performance. Il s'agit ici d'utiliser les informations sur la performance d'organisations similaires qui ont déjà mesuré leur performance, pour se faire une idée de la manière dont d'autres membres de la communauté procèdent.

4.3.3.5 Un exemple de la relation entre les objectifs de sécurité, les SPI et les SPT est illustré à la Figure 4-4. Dans cet exemple, l'organisation a enregistré 100 sorties de piste par million de mouvements en 2018. Il a été déterminé que ce chiffre était trop élevé et un objectif de réduire le nombre de sorties de piste de cinquante pour cent d'ici 2022 a été fixé. Des mesures ciblées spécifiques, assorties d'échéanciers, ont été définies pour atteindre ces cibles. Pour suivre et mesurer ses progrès et en rendre compte, l'organisation a choisi comme SPI « Sorties de piste par million de mouvements par an ». L'organisation est consciente que les progrès seront plus rapides et efficaces si des cibles spécifiques alignées sur l'objectif de sécurité sont fixées. Elle a donc fixé une cible de sécurité qui correspond à une réduction moyenne de 12,5 pour cent par an pour la période de compte rendu (quatre ans). Comme indiqué dans la représentation graphique, on s'attend à ce que les progrès soient plus importants dans les premières années et moindres ensuite. Ce profil d'évolution est représenté par la projection courbe vers l'objectif. Dans la Figure 4-4 :

a) l'objectif de sécurité SMART est « 50 pour cent de réduction des sorties de piste d'ici 2022 » ;

b) le SPI sélectionné est le « nombre de sorties de piste par million de mouvements par an » ;

c) les cibles de sécurité liées à cet objectif représentent des jalons pour atteindre l'objectif de sécurité SMART et correspondent à une réduction de ~12 pour cent par an jusqu'en 2022 :

1) la SPT 1a est « moins de 78 sorties de piste par million de mouvements en 2019 » ;

2) la SPT 1b est « moins de 64 sorties de piste par million de mouvements en 2020 » ;

3) la SPT 1c est « moins de 55 sorties de piste par million de mouvements en 2021 ».

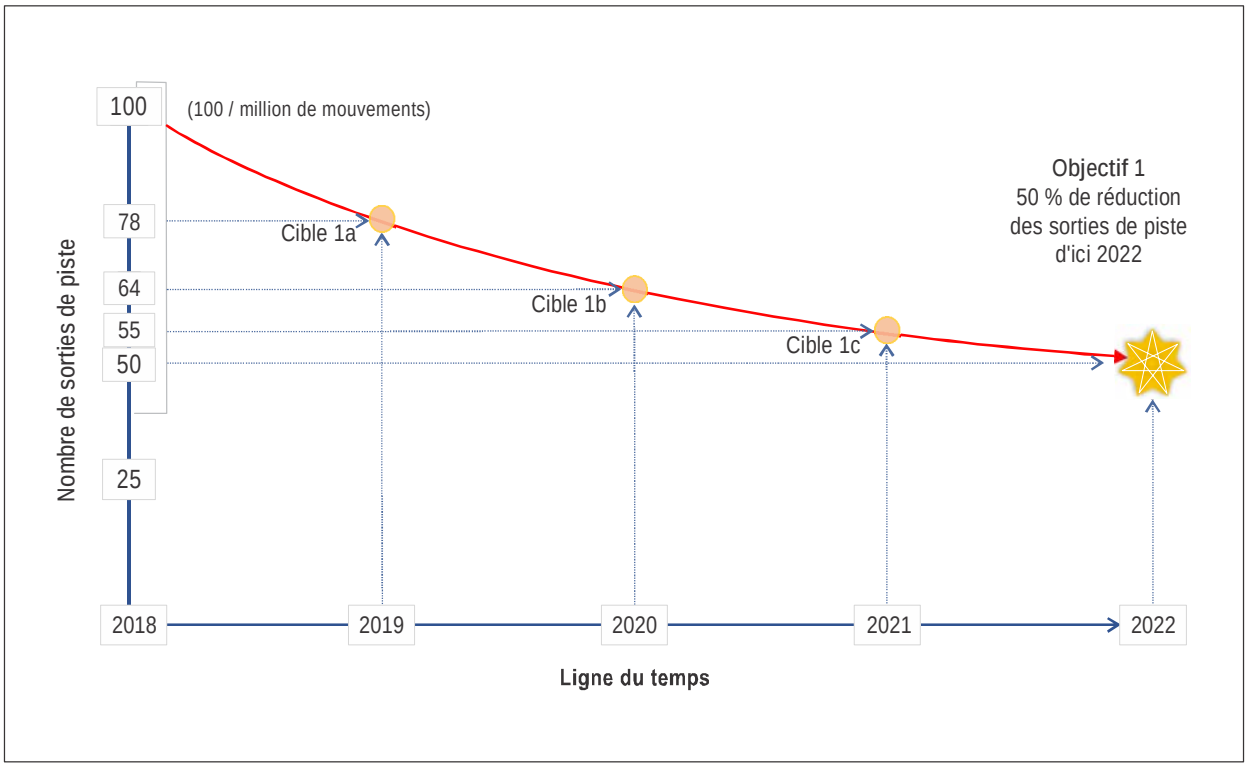

Figure 4-4. Exemple de SPT avec des objectifs de sécurité SMART

Autres considérations pour la sélection de SPI et de SPT

4.3.3.6 Lors de la sélection de SPI et de SPT, il convient de tenir également compte des points suivants :

a) *Gestion de la charge de travail*. Créer un nombre réaliste de SPI peut aider le personnel à gérer la charge de travail que nécessite le suivi et les comptes rendus qui y sont associés. Il en va de même pour la complexité des SPI ou pour la disponibilité des données requises. Il vaut mieux convenir de ce qui est faisable puis établir l'ordre de priorité pour la sélection des SPI sur cette base. Si un SPI n'alimente plus la performance de sécurité ou s'il reçoit une priorité moindre, il faut envisager de l'abandonner au profit d'un indicateur plus utile ou de plus haute priorité.

b) *Éventail optimal de SPI*. Une combinaison de SPI couvrant les domaines prioritaires permettra de comprendre la performance de sécurité générale de l'organisation et soutiendra un processus décisionnel fondé sur les données.

c) *Clarté des SPI*. Lors de la sélection d'un SPI, il faut avoir une idée claire de ce qui est mesuré et de la fréquence des mesures. Des SPI assortis de définitions claires aident à la compréhension des résultats, évitent les erreurs d'interprétation et permettent des comparaisons intéressantes au fil du temps.

d) *Encourager les comportements souhaités*. Les SPT peuvent modifier les comportements et contribuer à la réalisation des résultats souhaités. C'est particulièrement vrai si l'organisation attribue des récompenses, telles que des indemnités de gestion, lorsque la cible est atteinte. Les SPT devraient favoriser des comportements organisationnels et individuels positifs, volontairement axés sur la prise de décisions défendables et sur une amélioration de la performance de sécurité. Il est tout aussi important d'envisager les comportements involontaires potentiels lors de la sélection de SPI et de SPT.

e) *Choix de mesures utiles*. Il est essentiel de sélectionner des SPI utiles et pas seulement des SPI faciles à mesurer. Il appartient à l'organisation de décider des paramètres de sécurité les plus utiles, à savoir ceux qui amènent l'organisation à améliorer le processus décisionnel, la gestion de la performance de sécurité et la réalisation de ses objectifs de sécurité.

f) *Réalisation des SPT*. Il s'agit d'un aspect particulièrement important, lié aux comportements de sécurité souhaités. La réalisation de SPT convenues n'est pas toujours une indication d'amélioration de la performance de sécurité. L'organisation devrait établir une distinction entre la simple réalisation de SPT et une amélioration réelle, démontrable, de la performance de sécurité organisationnelle. Il est impératif que l'organisation envisage le contexte dans lequel la cible a été atteinte plutôt que d'analyser une SPT prise isolément. La reconnaissance d'une amélioration générale de la performance de sécurité plutôt que de la réalisation d'une SPT individuelle favorisera des comportements organisationnels souhaitables et encouragera l'échange d'informations de sécurité qui sont au cœur à la fois de la GRS et de l'assurance de la sécurité. Cela pourrait aussi renforcer la relation entre l'État et le prestataire de services et la volonté de l'un et l'autre de partager des données de sécurité et des idées.

Mises en garde pour la fixation de SPT

4.3.3.7 Il n'est pas toujours nécessaire ou approprié de définir des SPT car certains SPI peuvent se prêter mieux à la surveillance des tendances qu'à la détermination d'une cible. Les comptes rendus en matière de sécurité constituent un exemple où une cible fixée pourrait soit décourager les gens de signaler quoi que ce soit (si la cible est de ne pas dépasser une limite chiffrée) ou les encourager à signaler des choses insignifiantes pour atteindre une cible (si la cible est d'atteindre un certain chiffre). Certains SPI conviennent mieux pour définir un cap vers une amélioration continue de la performance de sécurité (p. ex. réduire le nombre d'événements) que pour définir une cible absolue, parfois difficile à déterminer. Les éléments suivants devraient aussi être pris en considération dans la détermination de SPT appropriées :

a) Risque de favoriser des comportements non souhaitables : si les dirigeants ou les organisations sont trop concentrés sur la réalisation de chiffres en tant qu'indicateurs de succès, ils pourraient ne pas atteindre l'amélioration souhaitée de la performance de sécurité.

b) Cibles opérationnelles : une priorité excessive accordée à la réalisation de cibles opérationnelles (telles que départs à l'heure, réduction des frais généraux, etc.) sans un contrepoids de SPT peut mener à « réaliser les cibles opérationnelles » sans nécessairement améliorer la performance de sécurité.

c) Focalisation sur la quantité plutôt que sur la qualité : cela peut encourager le personnel ou des services à atteindre la cible mais, ce faisant, à fournir des produits ou des services de piètre qualité.

d) Plafonnement de l'innovation : le fait d'atteindre une cible peut, involontairement, mener à un relâchement et générer une impression qu'aucune amélioration supplémentaire n'est nécessaire, de sorte qu'un relâchement de la vigilance peut s'installer.

e) Conflit au sein de l'organisation : des cibles peuvent engendrer des conflits entre les services et les organisations, qui se déchirent sur les responsabilités plutôt que de s'attacher à tenter de travailler ensemble.

4.3.4 Mesure de la performance de sécurité

Pour mesurer correctement la performance de sécurité, il faut décider comment mesurer au mieux la réalisation des objectifs de sécurité. Ce genre de décision varie d'un État à l'autre et d'un prestataire de services à l'autre. Les organisations devraient prendre le temps de développer leur perception stratégique de ce qui favorise l'amélioration de la sécurité pour atteindre leurs objectifs de sécurité.

4.3.5 Utilisation de SPI et de SPT

Les SPI et SPT peuvent être utilisés de différentes manières pour démontrer la performance de sécurité. Il est crucial que les organisations adaptent, sélectionnent et appliquent divers outils et approches de mesure en fonction de leurs circonstances spécifiques et de la nature de ce qu'il faut mesurer. Par exemple, dans certains cas, des organisations pourraient adopter des SPI qui sont tous associés à des SPT spécifiques. Dans d'autres cas, il pourrait être préférable de se concentrer sur la réalisation d'une tendance positive dans les SPI, sans valeurs cibles spécifiques. L'ensemble des paramètres de performance sélectionnés reposera généralement sur une combinaison de ces approches.

4.4 SUIVI DE LA PERFORMANCE DE SÉCURITÉ

4.4.1 Une fois qu'une organisation a identifié les cibles sur la base des SPI qu'elle considère à même de fournir le résultat prévu, elle doit s'assurer que les parties prenantes la suivront dans sa démarche en attribuant des responsabilités claires d'application. Une définition de SPT pour chaque autorité, secteur et prestataire de services de l'aviation soutient la réalisation de l'ALoSP pour l'État en attribuant des responsabilités claires.

4.4.2 Des mécanismes de suivi et de mesure de la performance de sécurité de l'organisation devraient être établis pour identifier quels changements pourraient être requis si les progrès engrangés ne sont pas conformes aux prévisions et pour renforcer l'engagement de l'organisation à atteindre ses objectifs de sécurité.

4.4.3 Performance de sécurité de référence

Pour comprendre comment l'organisation projette de progresser vers la réalisation de ses objectifs de sécurité, il faut que cette organisation sache où elle en est au chapitre de la sécurité. Une fois que la structure de la performance de sécurité de l'organisation (objectifs, indicateurs, cibles, alertes de sécurité) a été établie et fonctionne, il est possible de déterminer sa performance de sécurité de référence au moyen d'une période de suivi. La performance de sécurité de référence est la performance de sécurité au début du processus de mesure de la performance de sécurité, soit le point à partir duquel les progrès peuvent être mesurés. Dans l'exemple utilisé aux Figures 4-3 et 4-4, la performance de sécurité de référence pour cet objectif de sécurité spécifique était « 100 sorties de piste par million de mouvements pendant l'année (2018) ». Cette base solide permet de consigner des indications et des cibles précises et utiles.

4.4.4 Affinement des SPI et des SPT

4.4.4.1 Les SPI et les SPT qui y sont associées devront être réexaminés pour déterminer s'ils fournissent les informations requises pour suivre les progrès sur la voie de la réalisation des objectifs de sécurité et pour garantir que les cibles sont réalistes et réalisables.

4.4.4.2 La gestion de la performance de sécurité est une activité permanente. Les risques de sécurité et/ou la disponibilité des données changent au fil du temps. Les SPI initiaux peuvent être élaborés avec des ressources limitées pour ce qui est des informations de sécurité. Ultérieurement, on peut augmenter le nombre de canaux de compte rendu mis en place ainsi que la quantité de données de sécurité disponibles, et les capacités d'analyse de sécurité de l'organisation vont probablement atteindre leur maturité. Il peut être approprié pour les organisations d'élaborer au départ des SPI simples (plus larges). À mesure que les organisations collectent plus de données et accroissent leurs capacités de gestion de la sécurité, elles peuvent envisager d'affiner la portée des SPI et des SPT pour mieux les aligner sur les objectifs de sécurité souhaités. De petites organisations non complexes peuvent choisir d'affiner leurs SPI et leurs SPT et/ou de sélectionner des indicateurs génériques (mais spécifiques) qui s'appliquent à la plupart des systèmes d'aviation. Voici quelques exemples d'indicateurs génériques :

a) des événements au cours desquels des dommages structurels ont été causés à des équipements ;

b) des événements faisant apparaître des circonstances dans lesquelles un accident a failli se produire ;

c) des événements dans lesquels le personnel d'exploitation ou des membres de la communauté de l'aviation ont été mortellement ou grièvement blessés ;

d) des événements dans lesquels des membres du personnel d'exploitation ont été frappés d'incapacité ou ont été incapables d'exécuter leurs tâches en toute sécurité ;

e) le taux de comptes rendus volontaires d'événements ;

f) le taux de comptes rendus obligatoires d'événements.

4.4.4.3 De plus grandes organisations plus complexes peuvent choisir d'instaurer un éventail plus large et/ou plus approfondi de SPI et de SPT et d'intégrer des indicateurs génériques tels que ceux énumérés ci-dessus avec des indicateurs plus spécifiques à leurs activités. Un grand aéroport, par exemple, qui fournit des services à d'importantes compagnies aériennes et est situé sous un espace aérien complexe pourrait envisager de combiner certains des SPI génériques avec des SPI de portée plus affinée représentant des aspects spécifiques de son exploitation. Le suivi de ces indicateurs peut exiger de plus gros efforts mais produira sans doute de meilleurs résultats sur le plan de la sécurité. Il existe une corrélation claire entre la complexité relative des SPI et des SPT et l'ampleur et la complexité des opérations de l'État ou du prestataire de services. Cette complexité relative devrait être reflétée dans l'indicateur et dans la cible fixée. Les personnes responsables de la mise en place de la gestion de la performance de sécurité devraient en avoir conscience.

4.4.4.4 L'ensemble des SPI et des SPT sélectionnés par une organisation devraient être réexaminés régulièrement pour garantir qu'ils restent utiles en tant qu'indications de la performance de sécurité de l'organisation. Voici quelques raisons de maintenir, abandonner ou modifier des SPI et des SPT :

a) les SPI livrent continuellement la même valeur (notamment zéro pour cent ou 100 pour cent) ; il est peu probable que de tels SPI donnent des indications intéressantes pour le processus décisionnel de la haute direction ;

b) des SPI ont le même comportement et, en tant que tels, sont considérés comme des doublons ;

c) la SPT pour un SPI mis en œuvre pour mesurer l'introduction d'un programme ou d'une amélioration ciblée a été atteinte ;

d) une plus haute priorité de suivi et de mesure a été donnée à une autre préoccupation de sécurité ;

e) le but est de mieux comprendre un problème de sécurité particulier en cernant davantage les spécificités d'un SPI (p. ex. réduire le « bruit » pour clarifier le « signal ») ;

f) les objectifs de sécurité ont changé et, en conséquence, les SPI doivent être actualisés pour rester pertinents.

4.4.5 Facteurs déclencheurs en matière de sécurité

4.4.5.1 Il convient d'expliquer brièvement les notions de facteurs déclencheurs pour soutenir leur éventuel rôle dans le contexte de la gestion de la performance de sécurité d'une organisation.

4.4.5.2 Un facteur déclencheur est une valeur établie d'un niveau ou d'un critère qui sert à déclencher (commencer) une évaluation, une décision, un ajustement ou une action correctrice en rapport avec l'indicateur spécifique. Une méthode de fixation de critères de déclenchement pour dépassement des limites pour les SPT est l'utilisation du principe de l'écart type de la population (STDEVP). Cette méthode dérive la valeur de l'écart type (SD) à partir des points de données historiques précédents d'un indicateur de sécurité donné. La valeur de l'écart type plus la valeur de la moyenne de l'ensemble des données historiques constituent la valeur de déclenchement de base pour la période de suivi suivante. Le principe de l'écart type (une fonction statistique de base) fixe les critères de niveau de déclenchement sur la base de la performance historique réelle d'un indicateur donné (ensemble de données), y compris sa volatilité (fluctuations des points de données). Un ensemble de données historiques plus volatil produira généralement une valeur de niveau de déclenchement plus élevée (plus généreuse) pour la période de suivi suivante. Les facteurs déclencheurs donnent des alertes précoces qui permettent aux décideurs de prendre des décisions de sécurité en connaissance de cause et, donc, d'améliorer la performance de sécurité. Un exemple de niveaux de déclenchement basés sur les écarts types (SD) est donné à la Figure 4-5 ci-dessous. Dans cet exemple, il est possible que des décisions fondées sur les données et des mesures d'atténuation des risques de sécurité doivent être prises lorsque la tendance dépasse +1 SD ou +2 SD par rapport à la moyenne de la période précédente. Souvent les niveaux de déclenchement (dans ce cas +1 SD, +2 SD ou au-delà de +2 SD) seront alignés sur les niveaux de gestion des décisions et sur l'urgence de prendre des mesures.

4.4.5.3 Une fois que les SPT et les niveaux des facteurs déclencheurs (le cas échéant) ont été définis, les SPI qui y sont associés peuvent faire l'objet d'un suivi destiné à déterminer leurs performances respectives. Un résumé consolidé des résultats de la performance globale des SPT et des facteurs déclencheurs pour l'ensemble des SPI peut aussi être compilé et/ou agrégé pour une période de suivi donnée. Des valeurs qualitatives (satisfaisant/insatisfaisant) peuvent être attribuées à chaque réalisation de SPT et à chaque niveau de déclenchement non dépassé. Ou des valeurs chiffrées (points) peuvent être utilisées pour donner une mesure quantitative de la performance globale de l'ensemble des SPI.

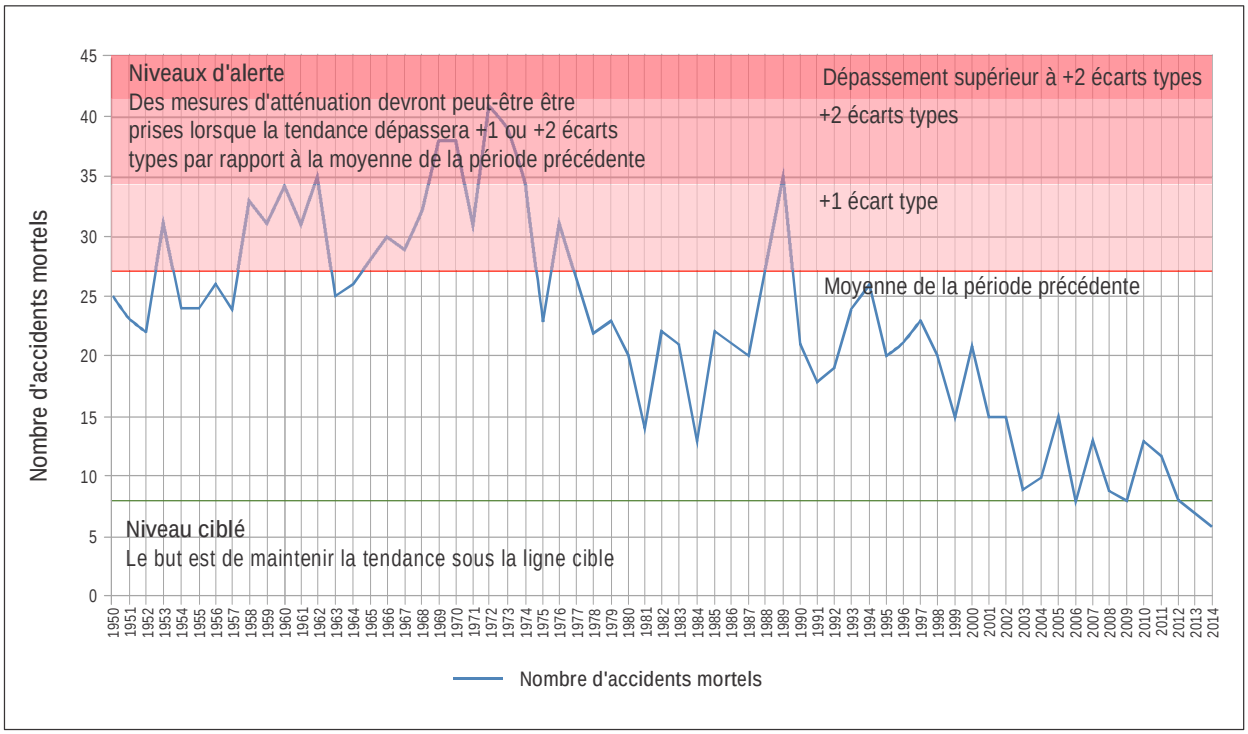

Figure 4-5. Exemple de représentation de niveaux de déclenchement en matière de sécurité (alertes)

4.4.5.4 Il convient de noter que les valeurs de déclenchement servent à déclencher (commencer) une évaluation, une décision, un ajustement ou une action correctrice en rapport avec l'indicateur spécifique. Le déclenchement d'un SPI n'est pas nécessairement catastrophique ni un signe d'échec. C'est seulement un signe que l'activité a dépassé la limite prédéterminée. Le facteur déclencheur vise à attirer l'attention des décideurs, qui sont maintenant en mesure de prendre ou non une mesure correctrice, en fonction des circonstances.

4.4.6 Avertissement sur les facteurs déclencheurs

4.4.6.1 L'identification de niveaux de déclenchement fiables soulève des difficultés. Les facteurs déclencheurs et les niveaux qui y sont associés fonctionnent très bien lorsqu'il existe beaucoup de données de sécurité et de capacités de gestion des données de sécurité. La gestion de ces données peut imposer une charge de travail supplémentaire à l'organisation. La notion de facteur déclencheur a été conçue pour et est surtout appropriée à une GRS de systèmes purement techniques (p. ex. le suivi des moteurs d'aviation). Dans ce cas, de grandes quantités de données quantitatives soutiennent l'identification de facteurs déclencheurs et de niveaux de déclenchement précis. On peut affirmer que la notion de facteurs déclencheurs est moins pertinente pour la GRS de systèmes sociotechniques. Les systèmes sociotechniques sont des systèmes où les personnes interagissent activement avec les processus et les technologies pour réaliser les objectifs de production ou de prestation de services du système. Tant les PNS que les SGS sont des systèmes sociotechniques. Les facteurs déclencheurs utilisés dans les systèmes sociotechniques sont moins fiables et moins utiles parce que la participation d'humains aux systèmes limite la possibilité d'effectuer des mesures fiables.

4.4.6.2 Une approche plus souple est donc nécessaire pour que les facteurs déclencheurs soient utiles. L'Annexe 19 n'exige pas des États ou des prestataires de services qu'ils définissent des niveaux de déclenchement pour chaque SPI. Toutefois, une définition de tels niveaux présente des avantages pour les organisations disposant de données très spécifiques pour un SPI, d'un nombre suffisant de points de données et de données suffisamment fiables.

4.4.6.3 La Figure 4-6 ci-dessous est une extension de l'exemple précédent, à savoir une « réduction de 50 pour cent des sorties de piste d'ici 2022 ». Dans ce scénario, nous sommes en 2020. L'organisation collecte des données de sécurité (SPI — « Aucune sortie de piste/million de mouvements/an ») et travaille avec les parties prenantes pour réduire les événements. La SPT pour 2019 (<78 sorties de piste/million de mouvements/an) a été atteinte. Toutefois, le SPI montre que non seulement la SPT pour 2020 (<64 sorties de piste/million de mouvements/an) n'a pas été atteinte, mais le nombre de sorties de piste a dépassé le niveau de déclenchement pendant deux périodes de compte rendu consécutives. Les décideurs ont été avertis de la détérioration de la performance de sécurité et sont en mesure de décider de prendre une ou plusieurs mesures supplémentaires sur la base des données. Leurs décisions fondées sur les données viseront à ramener la performance de sécurité dans la zone acceptable et sur la bonne voie pour réaliser l'objectif de sécurité.

4.4.7 Identification des actions requises

4.4.7.1 On peut affirmer que le résultat le plus important de la mise en place d'une structure de gestion de la performance de sécurité est la présentation d'informations aux décideurs de l'organisation afin que ceux-ci puissent prendre des décisions sur la base de données de sécurité et d'informations de sécurité actualisées et fiables. Le but devrait toujours être de prendre des décisions conformément à la politique de sécurité et dans la perspective de réaliser les objectifs de sécurité.

4.4.7.2 Dans le domaine de la gestion de la performance de sécurité, le processus décisionnel fondé sur les données consiste à prendre des décisions efficaces, en connaissance de cause, sur la base des résultats de SPI mesurés et suivis, ou d'autres comptes rendus et de l'analyse des données de sécurité et des informations de sécurité. L'utilisation de données de sécurité valables et pertinentes, combinées à des informations qui les contextualisent, aide l'organisation à prendre des décisions dans la droite ligne de ses objectifs et cibles de sécurité. Les renseignements contextuels peuvent aussi inclure les priorités d'autres parties prenantes, des lacunes connues dans les données et d'autres données complémentaires pour peser le pour et le contre et évaluer les possibilités, les limites et les risques liés à cette décision. La disponibilité et la facilité d'interprétation des informations contribuent à atténuer les partis pris, les influences et les erreurs humaines dans le processus décisionnel.

4.4.7.3 Le processus décisionnel fondé sur les données soutient aussi l'évaluation de décisions prises dans le passé pour soutenir le réalignement sur les objectifs de sécurité. De plus amples éléments d'orientation sur le processus décisionnel fondé sur les données sont fournis au Chapitre 6.

4.5 ACTUALISATION DES OBJECTIFS DE SÉCURITÉ

La gestion de la performance de sécurité n'a pas pour ambition de régler les choses une fois pour toutes. La gestion de la performance de sécurité est un processus dynamique au cœur du fonctionnement de chaque État et de chaque prestataire de services et elle devrait être réexaminée et actualisée :

a) régulièrement, conformément au cycle périodique établi et convenu par le comité de sécurité de haut niveau ;

b) sur la base des intrants provenant d'analyses de la sécurité (voir Chapitre 6 pour plus de détails) ;

c) en réponse à des changements majeurs dans les activités, les risques principaux ou l'environnement.

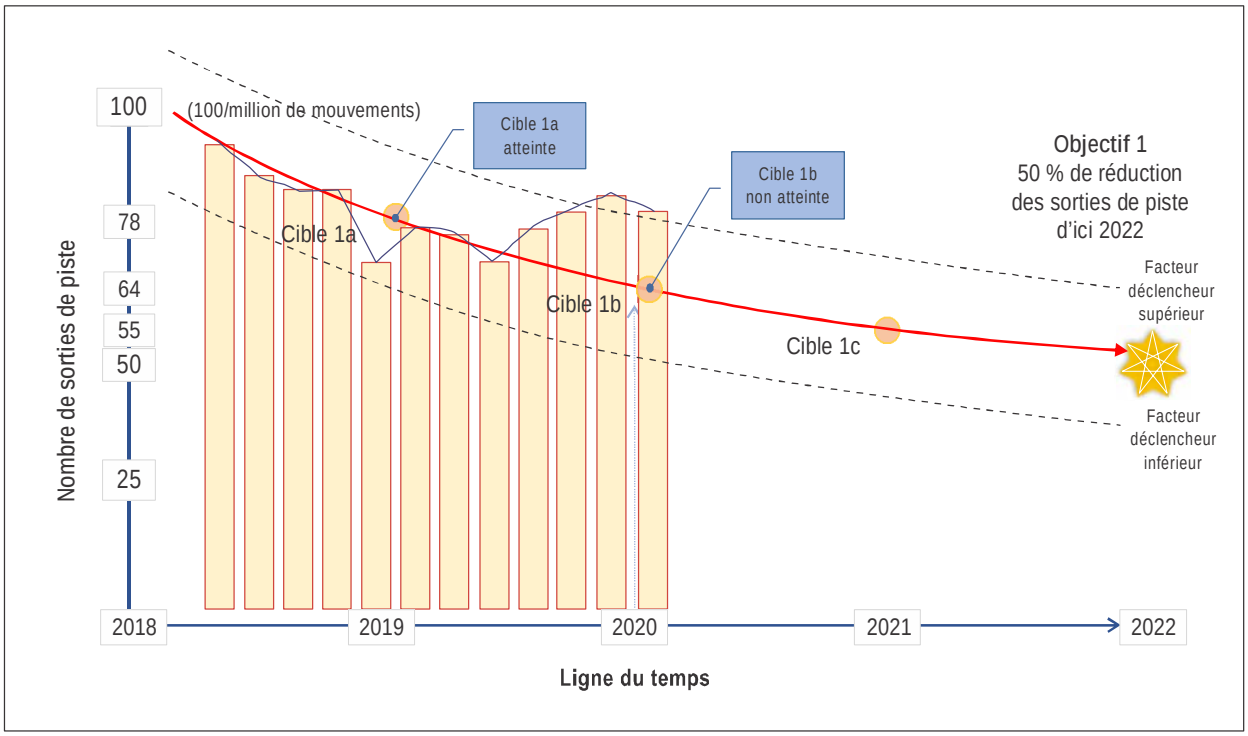

Figure 4-6. Exemple de fixation de niveaux de déclenchement en matière de sécurité

Chapitre 5

SYSTÈMES DE COLLECTE ET DE TRAITEMENT DES DONNÉES DE SÉCURITÉ

5.1 INTRODUCTION

5.1.1 La distinction entre données de sécurité et informations de sécurité apparaît dans les définitions données dans l'Annexe 19. Les données de sécurité sont les données initialement communiquées ou enregistrées à la suite d'une observation ou d'une mesure. Elles sont transformées en informations de sécurité lorsqu'elles sont traitées, organisées, intégrées ou analysées dans un contexte donné de manière à être utiles pour la gestion de la sécurité. Il est possible de continuer à traiter les informations de sécurité de diverses manières pour en extraire différentes significations.

5.1.2 L'efficacité de la gestion de la sécurité est fort tributaire de l'efficacité des capacités de collecte, d'analyse et de gestion générale des données de sécurité. Il est fondamental de disposer d'une base solide de données de sécurité et d'informations de sécurité pour assurer la gestion de la sécurité car c'est la base d'un processus décisionnel fondé sur les données. Des données de sécurité et des informations de sécurité fiables sont nécessaires pour identifier les tendances, prendre des décisions et évaluer la performance de sécurité par rapport aux cibles et aux objectifs de sécurité, et pour évaluer le risque.

5.1.3 L'Annexe 19 exige que les prestataires de services élaborent et tiennent à jour un processus formel pour collecter, enregistrer, prendre des mesures et donner des rétro-informations sur les dangers dans leurs activités, sur la base d'une combinaison de méthodes réactives et proactives de collecte de données de sécurité.

5.1.4 De même, le Chapitre 8 de l'Annexe 13 — *Enquêtes sur les accidents et incidents d'aviation* stipule que les États établiront et tiendront à jour une base de données sur les accidents et incidents, pour faciliter l'analyse efficace des renseignements sur les carences réelles ou potentielles en matière de sécurité ainsi que pour déterminer les mesures préventives qui peuvent être nécessaires.

5.1.5 L'Annexe 19 exige que les États mettent en place des systèmes de collecte et de traitement des données de sécurité (SDCPS) pour effectuer la saisie, le stockage et l'agrégation des données de sécurité et des informations de sécurité et en permettre l'analyse, afin de soutenir leurs activités de gestion de la performance de sécurité. L'abréviation SDCPS est un terme générique utilisé pour désigner les systèmes de traitement et de compte rendu de données, les bases de données, les mécanismes d'échange d'informations de sécurité et les informations enregistrées. L'expression « base de données de sécurité » peut désigner une base de données unique ou des bases de données multiples. Il est recommandé que les autorités nationales responsables de la mise en œuvre du PNS aient accès aux SDCPS pour soutenir leurs responsabilités en matière de sécurité.

5.1.6 Les prestataires de services doivent aussi élaborer et tenir à jour les moyens nécessaires pour vérifier leur performance de sécurité en rapport avec leurs SPI et leurs SPT, à l'appui de leurs objectifs de sécurité, au moyen des SDCPS. Ces moyens peuvent être basés sur des méthodes réactives et proactives de collecte de données de sécurité et d'informations de sécurité.

5.1.7 Les orientations présentées dans ce chapitre sont valables tant pour les États que pour les prestataires de services et visent à garantir que les données de sécurité et les informations de sécurité collectées permettent une prise de décisions efficace et valable.

5.1.8 Les organisations devraient s'assurer qu'elles ont du personnel qualifié pour collecter et stocker des données de sécurité, et les compétences requises pour traiter ces données. À cet égard, elles doivent pouvoir disposer d'individus hautement compétents en technologies de l'information et maîtrisant les besoins de données, la normalisation des données, la collecte et le stockage des données, la gouvernance des données et la capacité de comprendre les demandes d'informations potentielles pouvant être requises pour l'analyse. De plus, l'organisation devrait s'assurer que chaque SDCPS a son responsable désigné, chargé d'appliquer aux données de sécurité, aux informations de sécurité et aux sources connexes la protection prévue à l'Appendice 3 de l'Annexe 19. Le Chapitre 7 contient de plus amples informations.

5.2 COLLECTE DES DONNÉES DE SÉCURITÉ ET DES INFORMATIONS DE SÉCURITÉ

5.2.1 Objectifs aux différents niveaux du système aéronautique

5.2.1.1 Depuis les années 1970, l'OACI introduit, dans les Annexes, les Procédures pour les services de navigation aérienne (PANS) et les documents, des dispositions qui demandent aux États de mettre en place des systèmes de compte rendu pour la collecte de données de sécurité et d'informations de sécurité. La plupart de ces dispositions concernent des systèmes de compte rendu de sécurité spécifiques au secteur, à l'exception de l'Annexe 13, qui vise spécifiquement les comptes rendus d'accidents et d'incidents graves. Les dispositions relatives aux systèmes de compte rendu obligatoire et volontaire figurant dans l'Annexe 19 proviennent de l'Annexe 13.

5.2.1.2 Nombre de prestataires de services ont recueilli un vaste éventail de données de sécurité et d'informations de sécurité, notamment au moyen de systèmes de compte rendu obligatoire et volontaire en matière de sécurité et de systèmes automatisés de saisie de données. Ces données de sécurité et informations de sécurité permettent aux prestataires de services d'identifier les dangers et servent de base aux activités de gestion de la performance de sécurité au niveau du prestataire de services. Le partage d'informations de sécurité comporte de nombreux avantages, en particulier pour ce qui est de l'identification des dangers qu'un prestataire de services ne peut percevoir à lui seul. Des indications sur le partage et l'échange d'informations de sécurité figurent au Chapitre 6.

5.2.1.3 L'Annexe 19 exige que les États mettent en place des SDCPS pour effectuer la saisie, le stockage et l'agrégation des données de sécurité et des informations de sécurité et en permettre l'analyse, afin de soutenir l'identification des dangers qui concernent l'ensemble du système aéronautique. Les implications de cette exigence dépassent le simple accès permettant de visionner les données aux fins du suivi de la performance de sécurité des prestataires de services. De plus, la mise en place de systèmes de compte rendu et de bases de données pour la collecte de données de sécurité et d'informations de sécurité ne suffit pas pour garantir la disponibilité des données de sécurité nécessaires pour permettre l'analyse. Les États doivent aussi adopter des lois, réglementations, processus et procédures pour garantir que les données de sécurité et informations de sécurité identifiées dans l'Annexe 19 soient communiquées et collectées auprès des prestataires de services et d'autres parties prenantes pour alimenter les SDCPS. Dès lors, les protections prévues à l'Annexe 19, Appendice 3, doivent être en place pour garantir l'utilisation des données de sécurité et des informations de sécurité aux fins de maintenir ou d'améliorer la sécurité. Des arrangements peuvent aussi être mis en place pour qu'un tiers collecte, stocke et analyse les données de sécurité et les informations de sécurité au nom de l'État. Des indications sur la protection des données de sécurité et des informations de sécurité figurent au Chapitre 7.

5.2.1.4 De plus, les données de sécurité et les informations de sécurité doivent être collectées, stockées et analysées au niveau régional par les groupes régionaux de sécurité de l'aviation (RASG) pour faciliter l'identification des dangers qui transcendent les frontières nationales et pour promouvoir les efforts de collaboration aux fins d'atténuer les risques de sécurité.

5.2.2 Détermination des données et informations à collecter

5.2.2.1 Chaque organisation doit déterminer quelles données de sécurité et quelles informations de sécurité elle doit collecter pour soutenir son processus de gestion de la performance de sécurité et prendre des décisions en matière de sécurité. Les besoins en données de sécurité et en informations de sécurité peuvent être déterminés au moyen d'une approche descendante et/ou ascendante. Le choix de l'approche peut être influencé par différentes considérations, telles que les conditions et priorités nationales et locales ou la nécessité de fournir ces données pour soutenir le suivi des SPI.

5.2.2.2 L'identification et la collecte des données de sécurité devraient être alignées sur le besoin de l'organisation de gérer efficacement la sécurité. Dans certains cas, le processus de GRS fera ressortir le besoin de données de sécurité supplémentaires pour mieux évaluer l'incidence (le niveau de probabilité et de gravité) et pour déterminer les risques qui y sont associés. De même, le processus de gestion de la performance de sécurité peut faire ressortir un besoin d'informations supplémentaires pour permettre une compréhension plus complète d'un problème particulier de sécurité ou pour faciliter l'établissement ou l'affinement de SPI.

5.2.2.3 Il faut tenir compte de possibles biais lorsque l'on collecte et utilise des données de sécurité et des informations de sécurité. Par exemple, les termes utilisés dans des comptes rendus volontaires peuvent parfois être émotifs ou destinés à atteindre les objectifs d'un individu, objectifs qui ne sont pas nécessairement dans l'intérêt de l'ensemble de l'organisation. Dans ces cas, les informations devraient être utilisées avec discernement.

5.2.2.4 Les États et les prestataires de services devraient envisager d'adopter une approche intégrée pour la collecte de données de sécurité provenant de différentes sources, tant internes qu'externes. L'intégration permet aux organisations d'obtenir une idée plus précise de leurs risques de sécurité et de la mesure dans laquelle l'organisation atteint ses objectifs de sécurité. Il convient de noter que des données de sécurité et des informations de sécurité qui paraissent à première vue non liées peuvent ultérieurement s'avérer cruciales pour identifier des problèmes de sécurité et soutenir un processus décisionnel fondé sur les données.

5.2.2.5 Il est souhaitable de rationaliser la quantité de données de sécurité et d'informations de sécurité en identifiant celles qui soutiennent spécifiquement la gestion efficace de la sécurité au sein de l'organisation. Les données de sécurité et les informations de sécurité collectées devraient soutenir la mesure fiable de la performance du système et l'évaluation des risques connus, ainsi que l'identification des risques émergents, dans les limites des activités de l'organisation. Les données de sécurité et les informations de sécurité requises seront influencées par la taille et la complexité des activités de l'organisation.

5.2.2.6 La Figure 5-1 donne des exemples de données de sécurité et d'informations de sécurité types qui sont, dans bien des cas, déjà disponibles. La coordination entre les services ou les divisions est nécessaire pour rationaliser les efforts de compte rendu et de collecte de données de sécurité, afin d'éviter les doublons.

5.2.3 Enquêtes sur les accidents et les incidents

L'Annexe 13 exige que les États établissent et tiennent à jour une base de données sur les accidents et incidents, pour faciliter l'analyse efficace des renseignements sur les carences réelles ou potentielles en matière de sécurité ainsi que pour déterminer les mesures préventives qui peuvent être nécessaires. Les autorités nationales responsables de la mise en œuvre du PNS devraient avoir accès à la base de données nationale sur les accidents et incidents pour leur permettre d'assumer leurs responsabilités en matière de sécurité. Des renseignements supplémentaires sur lesquels fonder des mesures préventives peuvent figurer dans les rapports d'enquête finals sur les accidents et incidents qui ont fait l'objet d'une enquête.

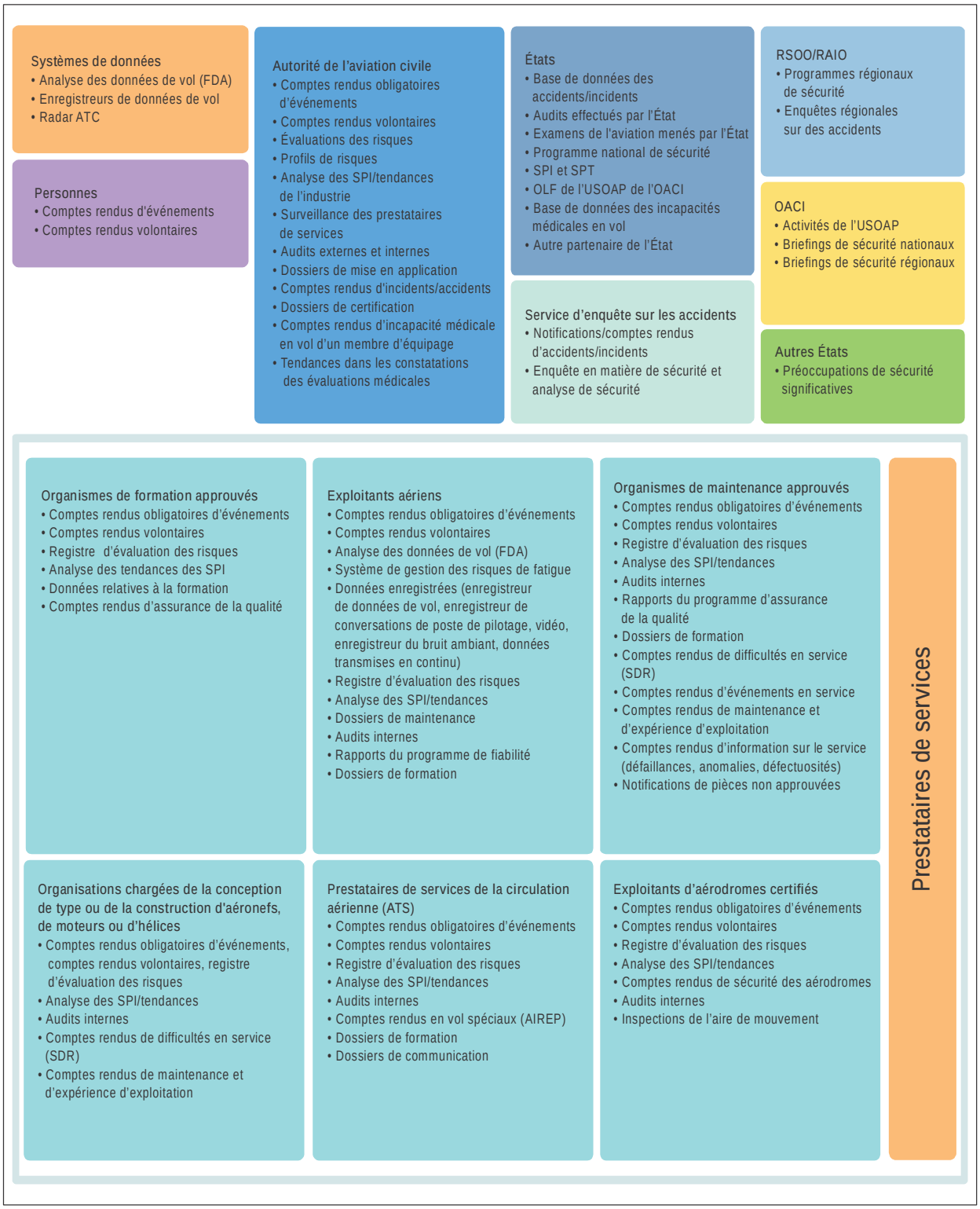

Figure 5-1. Sources classiques de données de sécurité et d'informations de sécurité

5.2.4 Enquêtes de sécurité menées par les autorités nationales ou par les prestataires de services aéronautiques

5.2.4.1 En application des dispositions de l'Annexe 13, les États doivent enquêter sur les accidents ainsi que sur les incidents graves survenus sur leur territoire et concernant des aéronefs d'une masse maximale supérieure à 2 250 kg. Ces enquêtes sont menées par le service d'enquête sur les accidents (AIA) de l'État, conformément aux dispositions de l'Annexe 13. La conduite de telles enquêtes peut être déléguée à un autre État ou à une organisation régionale d'enquête sur les accidents et incidents (RAIO) par accord et consentement mutuels.

5.2.4.2 Des enquêtes de sécurité autres que celles qu'exige l'Annexe 13 sont encouragées car elles fournissent des informations de sécurité utiles à l'appui de l'amélioration de la performance de sécurité. De plus amples informations sur les enquêtes de sécurité des prestataires de services figurent au Chapitre 9.

5.2.5 Systèmes de compte rendu obligatoire en matière de sécurité

5.2.5.1 L'Annexe 19 exige que les États établissent un système de compte rendu obligatoire qui inclut, sans toutefois s'y limiter, les comptes rendus d'incidents. Les systèmes de compte rendu élaborés par les États et les prestataires de services devraient être de la plus grande simplicité possible pour ce qui est de la création et de la soumission de comptes rendus obligatoires et de l'accès à ces derniers. Les systèmes de compte rendu obligatoire en matière de sécurité devraient viser à saisir tous les renseignements utiles sur un événement, notamment ce qui s'est passé, où, quand et à qui le compte rendu est adressé. De plus, les systèmes de compte rendu obligatoire en matière de sécurité devraient prévoir la saisie de certains dangers spécifiques dont on sait qu'ils contribuent à des accidents, dangers dont l'identification et la communication en temps utile sont considérées comme précieuses (p. ex. conditions météorologiques régulières, activité volcanique, etc.).

5.2.5.2 Indépendamment de la portée du ou des systèmes de compte rendu obligatoire, il est recommandé que tous les comptes rendus à collecte obligatoire soient protégés conformément aux principes exposés en détail au Chapitre 7.

5.2.5.3 Les systèmes de compte rendu obligatoire d'événements tendent à collecter plus de renseignements techniques (p. ex. défaillances du matériel) que d'aspects relatifs à la performance humaine. Pour répondre à la nécessité d'élargir l'éventail de comptes rendus en matière de sécurité, les États devraient aussi mettre en œuvre un système de compte rendu volontaire en matière de sécurité. Le but est de recueillir plus de renseignements, notamment sur des aspects liés aux facteurs humains, et de renforcer la sécurité de l'aviation.

Comptes rendus d'accidents et d'incidents

5.2.5.4 Toutes les parties prenantes de l'aviation sont concernées par les comptes rendus d'accidents et d'incidents. Le personnel d'exploitation doit rendre compte d'accidents et de certains types d'incidents dès que possible à l'AIA de l'État et par le moyen le plus rapide disponible. Les incidents graves doivent être notifiés ; une liste d'exemples d'incidents susceptibles d'être graves figure dans le Supplément C à l'Annexe 13.

5.2.5.5 Voici deux aspects principaux à envisager pour décider si un incident doit être classé comme grave :

a) Des circonstances indiquent-elles qu'il y a eu une forte probabilité d'accident ?

b) L'accident a-t-il été évité uniquement par chance ?

5.2.6 Systèmes de compte rendu volontaire en matière de sécurité

5.2.6.1 Des systèmes de compte rendu volontaire en matière de sécurité devraient être établis pour collecter des données de sécurité et des informations de sécurité non saisies par le système de compte rendu obligatoire. Ces comptes rendus vont au-delà des comptes rendus classiques d'incidents. Les comptes rendus volontaires tendent à mettre en lumière des conditions latentes, telles que des procédures ou des réglementations de sécurité inappropriées, des erreurs humaines, etc. Les comptes rendus volontaires constituent une façon d'identifier les dangers.

5.2.6.2 Les États devraient accorder une protection aux données de sécurité saisies par les systèmes de compte rendu volontaire en matière de sécurité et les sources connexes, et aux informations de sécurité tirées de ces systèmes et sources. Il est conseillé aux États et aux prestataires de services de lire le Chapitre 7 pour obtenir des orientations sur la façon d'appliquer cette protection aux données de sécurité, aux informations de sécurité et aux sources connexes. L'application appropriée d'une telle protection garantira la disponibilité en continu de données de sécurité et d'informations de sécurité. Les États devraient aussi étudier les moyens de promouvoir des comptes rendus volontaires.

5.2.7 Dispositions spécifiques au secteur pour les comptes rendus en matière de sécurité

Les dispositions des systèmes de compte rendu en matière de sécurité ne cessent d'évoluer. De nouvelles exigences de compte rendu, non spécifiques au secteur, notamment concernant la fatigue et les systèmes d'aéronefs télépilotés (RPAS), ont été introduites plus récemment pour répondre à des préoccupations de sécurité spécifiques et à des activités émergentes dans le secteur de l'aviation. Le Tableau 7 fournit quelques exemples de systèmes de compte rendu spécifiques au secteur inclus dans diverses Annexes, PANS et documents.

Tableau 7. Exemples de systèmes de compte rendu spécifiques au secteur inclus dans diverses Annexes, PANS et documents

Système de compte rendu	*Référence*	*Pour l'État/ le prestataire de services*	*Année d'adoption/ approbation initiale*
Comptes rendus d'enquêtes sur les accidents et incidents d'aviation	Annexe 13 — *Enquêtes sur les accidents et incidents d'aviation*	État	1951
Comptes rendus d'incidents de circulation aérienne	PANS-ATM (Doc 4444), *Procédures pour les services de navigation aérienne — Gestion du trafic aérien*	État et prestataire de services	1970
Comptes rendus d'accidents et incidents concernant des marchandises dangereuses	Annexe 18 — *Sécurité du transport aérien des marchandises dangereuses*	État	1981
Comptes rendus de difficultés constatées en service	Annexe 8 — *Navigabilité des aéronefs*	État	1982
Comptes rendus d'incidents de circulation aérienne	Doc 9426, *Manuel de planification des services de la circulation aérienne,* 2e Partie	Prestataire de services	1984
Comptes rendus d'impacts d'oiseaux/animaux	Doc 9332, *Manuel du système OACI d'information sur les impacts d'oiseaux (IBIS)*	Prestataire de services	1989

Système de compte rendu	*Référence*	*Pour l'État/ le prestataire de services*	*Année d'adoption/ approbation initiale*
	Annexe 14 — *Aérodromes,* Volume I — *Conception et exploitation technique des aérodromes*	État et prestataire de services	1990
	Doc 9137, *Manuel des services d'aéroport*, Partie 3 — *Prévention et atténuation du risque faunique*	État et prestataire de services	1991
Comptes rendus d'incident d'exposition à un faisceau laser	Doc 9815, *Manuel sur les émetteurs laser et la sécurité des vols*	État	2003
Comptes rendus de fatigue	Annexe 6 — *Exploitation technique des aéronefs,* Partie 1 — *Aviation de transport commercial international — Avions*	Prestataire de services	2011
	Doc 9966, *Manuel pour la supervision des approches de gestion de la fatigue*	Prestataire de services	2012
Comptes rendus de difficultés constatées en service	Doc 9760, *Manuel de navigabilité*	État	2014
Comptes rendus de sécurité des aérodromes	Doc 9981, *Procédures pour les services de navigation aérienne (PANS) — Aérodromes*	Prestataire de services	2014
Systèmes d'aéronefs télépilotés (RPAS)	Doc 10019, *Manuel sur les systèmes d'aéronef télépiloté (RPAS)*	Prestataire de services	2015
Événements d'incapacité soudaine en vol et constatations d'évaluations médicales	Annexe 1 — *Licences du personnel*	État	2016
Comptes rendus d'accidents et incidents concernant des marchandises dangereuses	Doc 9284, *Instructions techniques pour la sécurité du transport aérien des marchandises dangereuses*	État et prestataire de services	2017

5.2.8 Systèmes de compte rendu par autodivulgation

Les systèmes des prestataires de services pour la collecte de données de sécurité au moyen de systèmes de compte rendu par autodivulgation, notamment la saisie automatique de données telles que le programme d'action pour la sécurité de l'aviation (ASAP) et les programmes FDA (programme d'assurance de la qualité des opérations aériennes [FOQA], programme d'audits de sécurité en service de ligne [LOSA] et enquêtes sur la sécurité des vols normaux [NOSS]), sont autant d'exemples de systèmes qui saisissent des données de sécurité par des observations directes d'équipages de conduite ou de contrôleurs de la circulation aérienne, respectivement. Tous ces systèmes permettent l'enregistrement des bonnes performances des humains et des systèmes. Voir le Chapitre 7 pour plus d'informations sur la protection des données de sécurité et des informations de sécurité saisies par des systèmes de compte rendu par autodivulgation et leurs sources.

5.2.9 Résultats d'inspections, d'audits ou d'enquêtes

Les résultats d'interactions entre des représentants de l'État et des prestataires de services, tels que les résultats d'inspections, d'audits ou d'enquêtes, peuvent aussi constituer des contributions utiles à l'ensemble des données de sécurité et des informations de sécurité. Les données de sécurité et les informations de sécurité tirées de ces interactions peuvent être utilisées comme preuves de l'efficacité du programme de surveillance lui-même.

5.2.10 Collecte optimale de données de sécurité et d'informations de sécurité

Une grande partie des données de sécurité et des informations de sécurité utilisées comme base du processus décisionnel fondé sur les données proviennent d'opérations quotidiennes courantes et sont disponibles au sein même de l'organisation. L'organisation devrait d'abord établir à quelle question spécifique les données de sécurité et les informations de sécurité sont censées répondre ou quel problème il faut résoudre. Cela permettra de déterminer la source appropriée et de clarifier la quantité de données ou d'informations requises.

5.3 TAXONOMIES

5.3.1 Les données de sécurité devraient idéalement être classées selon des taxonomies et des définitions d'appui, afin que les données puissent être saisies et stockées sur la base de termes utiles. Les taxonomies et définitions courantes établissent un langage normalisé, ce qui améliore la qualité de l'information et de la communication. La capacité de la communauté aéronautique à se concentrer sur des problèmes de sécurité est considérablement renforcée par le partage d'un langage commun. Les taxonomies permettent l'analyse et facilitent le partage et l'échange d'informations. Voici quelques exemples de taxonomies :

a) Modèle d'aéronef : L'organisation peut constituer une base de données de tous les modèles d'aéronefs certifiés pour voler.

b) Aéroport : L'organisation peut utiliser les codes de l'OACI ou de l'Association du transport aérien international (IATA) pour identifier les aéroports.

c) Type d'événement : Une organisation peut utiliser des taxonomies élaborées par l'OACI et par d'autres organisations internationales pour classifier les événements.

5.3.2 Il existe dans le secteur plusieurs taxonomies aéronautiques communes. En voici quelques exemples :

a) ADREP : taxonomie de catégories d'événements qui fait partie du système de comptes rendus d'accidents et d'incidents de l'OACI. Il s'agit d'une compilation de caractéristiques et de valeurs qui y sont associées qui permet une analyse des tendances en matière de sécurité dans ces catégories.

b) Équipe de taxonomie commune CAST (Équipe pour la sécurité de l'aviation commerciale)/OACI (Organisation de l'aviation civile internationale) (CICTT) : chargée d'élaborer des taxonomies et définitions communes pour les systèmes de comptes rendus d'accidents et d'incidents d'aviation.

c) Groupe de travail sur les indicateurs de performance de sécurité (SPI-TF) : chargé d'élaborer des métriques harmonisées au niveau mondial pour les SPI des prestataires de services dans le cadre des SGS de ces prestataires, afin d'assurer l'uniformité de la collecte d'informations et la comparaison des résultats d'analyse.

5.3.3 Un extrait de la taxonomie de la CICTT est fourni au Tableau 8 à titre d'exemple uniquement.

Tableau 8. Exemple de taxonomie type

Type d'opération	*Activité/ infrastructure/ système*	*Valeur*
Aérodrome, fournisseur de services de navigation aérienne, exploitant aérien, organisme de maintenance, organisme de conception et de construction	Autorité de réglementation	Législation et/ou réglementations inexistantes, mauvaises ou inefficaces
		Capacités d'enquête sur les accidents inexistantes ou inefficaces
		Capacités de supervision inadéquates
	Cadres dirigeants	Engagement limité ou inexistant de la direction — La direction ne fait pas preuve de soutien en faveur de l'activité.
		Description incomplète ou inexistante des rôles, obligations de rendre compte et responsabilités
		Disponibilité ou planification des ressources limitée ou absente, y compris en matière de dotation en personnel
		Politiques inefficaces ou inexistantes
		Procédures, instructions comprises, incomplètes ou incorrectes
		Mauvaises relations de travail et avec la direction ou absence de telles relations
		Structure organisationnelle inefficace ou inexistante
		Mauvaise culture organisationnelle de la sécurité
		Procédures d'audit inefficaces ou inexistantes
		Affectation des ressources limitée ou inexistante

5.3.4 Les taxonomies des dangers sont particulièrement importantes. L'identification d'un danger est souvent la première étape du processus de gestion du risque. L'utilisation dès le départ d'un langage communément accepté rend les données de sécurité plus utiles, plus faciles à classer et plus simples à traiter. La structure d'une taxonomie des dangers peut inclure une composante générique et une composante spécifique.

5.3.5 La composante générique permet aux utilisateurs de saisir la nature d'un danger en vue de faciliter son identification, son analyse et son codage. La CICTT a élaboré une taxonomie de haut niveau des dangers qui classe les dangers en familles de types de dangers (environnemental, technique, organisationnel et humain).

5.3.6 La composante spécifique précise davantage la définition et le contexte du danger. Cela permet un traitement plus détaillé de la gestion du risque. Les critères suivants peuvent être utiles pour la formulation des définitions des dangers. Un danger mentionné doit être :

a) clairement identifiable ;

b) décrit dans l'état désiré (maîtrisé) ;

c) identifié à l'aide de noms acceptés.

5.3.7 Il est possible que des taxonomies courantes ne soient pas toujours disponibles entre bases de données. Dans ce cas, un mappage des données devrait être utilisé pour permettre la normalisation des données de sécurité et des informations de sécurité, sur la base d'une équivalence. Si nous prenons l'exemple d'un type d'aéronef, un mappage de données pourrait montrer qu'un « Boeing 787-8 » dans une base de données est équivalent à un « 788 » dans une autre. Ce processus n'est pas toujours simple car le niveau de détail pendant la saisie des données de sécurité et des informations de sécurité peut être différent. La plupart des SDCPS sont configurés pour faciliter la normalisation de la saisie des données, ce qui allège la tâche de mappage des données.

5.4 TRAITEMENT DES DONNÉES DE SÉCURITÉ

Le traitement des données de sécurité désigne la manipulation des données de sécurité pour produire des informations de sécurité intéressantes, dans des formats utiles, tels que des diagrammes, des rapports ou des tableaux. Plusieurs aspects importants sont à prendre en considération dans le traitement des données de sécurité, notamment la qualité, l'agrégation, la fusion et le filtrage des données.

5.4.1 Qualité des données

5.4.1.1 La qualité des données fait référence à des données épurées et appropriées au but recherché. La qualité des données couvre les aspects suivants :

a) propreté ;

b) pertinence ;

c) opportunité ;

d) précision et exactitude.

5.4.1.2 Le nettoyage des données est le processus visant à détecter et corriger (ou éliminer) des saisies altérées ou inexactes dans un ensemble de données, un tableau ou une base de données et couvre l'identification de parties incomplètes, incorrectes, inexactes ou non pertinentes des données et le remplacement, la modification ou la suppression des données douteuses ou imprécises.

5.4.1.3 Les données pertinentes sont des données qui répondent aux besoins de l'organisation et représentent ses problèmes les plus importants. Une organisation devrait évaluer la pertinence des données sur la base de ses besoins et de ses activités.

5.4.1.4 L'opportunité des données de sécurité et des informations de sécurité est fonction de leur actualité. Les données utilisées pour des décisions devraient refléter ce qui se passe en temps quasi réel. Il faut souvent faire preuve de discernement sur la base de la volatilité de la situation. Par exemple, des données collectées il y a deux ans sur un type d'aéronef effectuant encore des vols sur la même route, sans modifications significatives, peuvent donner une image opportune de la situation. Par contre, les données collectées il y a une semaine sur un type d'aéronef qui n'est plus en service ne fourniront peut-être pas une image opportune, utile, de la réalité actuelle.

5.4.1.5 Par exactitude des données, on entend que les valeurs sont correctes et reflètent le scénario particulier qui est décrit. Une inexactitude des données se produit généralement lorsque des utilisateurs saisissent la mauvaise valeur ou commettent une coquille. Il est possible de résoudre ce problème en ayant du personnel qualifié et formé pour la saisie des données ou en prévoyant dans l'application des composants tels qu'un correcteur orthographique. Les valeurs des données peuvent devenir inexactes au fil du temps ; on parle alors de « détérioration des données ». Les mouvements sont une autre cause d'inexactitude de données. À mesure que les données sont extraites, transformées

et déplacées d'une base de données à l'autre, elles peuvent s'altérer dans une certaine mesure, surtout si le logiciel n'est pas solide.

5.4.2 Agrégation des données de sécurité et des informations de sécurité

On parle d'agrégation des données lorsque des données de sécurité et des informations de sécurité sont rassemblées et stockées dans le SDCPS de l'organisation et exprimées sous forme de résumé à des fins d'analyse. Agréger des données de sécurité et des informations de sécurité, c'est les collecter ensemble, ce qui produit un plus vaste ensemble de données. Dans le cas de SDCPS, les différents éléments des données de sécurité sont agrégés dans une base de données sans qu'aucun de ces éléments ne soit privilégié par rapport aux autres. Un but courant d'agrégation est d'obtenir des informations sur un groupe ou un type particulier d'activités sur la base de variables spécifiques telles que le lieu, le type de flotte ou le groupe professionnel. Il peut parfois être utile d'agréger les données de plusieurs organisations ou régions qui n'ont pas assez de données pour garantir une anonymisation appropriée afin de protéger les sources de données de sécurité et d'informations de sécurité et de soutenir l'analyse.

5.4.3 Fusion de données

La fusion de données est le processus consistant à fusionner de multiples ensembles de données pour produire des données de sécurité plus cohérentes, corrélées et utiles que celles qui sont fournies par un ensemble unique de données de sécurité. L'intégration d'ensembles de données de sécurité suivie d'une réduction ou d'un remplacement améliore la fiabilité et la convivialité desdites données. Par exemple, des données de systèmes FDA d'exploitants aériens pourraient être fusionnées avec des données météorologiques et des données radar pour obtenir un ensemble de données plus utile pour traitement ultérieur.

5.4.4 Filtrage des données de sécurité et des informations de sécurité

Le filtrage des données de sécurité couvre une vaste gamme de stratégies ou de solutions pour affiner les ensembles de données de sécurité. Il permet d'affiner les ensembles de données pour obtenir uniquement les données dont le décideur a besoin, sans inclure d'autres données qui peuvent être répétitives, non pertinentes, voire sensibles. Différents types de filtres de données peuvent être utilisés pour générer des rapports ou présenter les données sous des formes qui facilitent la communication.

5.5 GESTION DES DONNÉES DE SÉCURITÉ ET DES INFORMATIONS DE SÉCURITÉ

5.5.1 La gestion des données de sécurité et des informations de sécurité peut être définie comme l'élaboration, l'exécution et la supervision de plans, politiques, programmes et pratiques qui garantissent l'intégrité, la disponibilité, la convivialité et la protection générales des données de sécurité et des informations de sécurité utilisées par l'organisation.

5.5.2 La gestion des données de sécurité et des informations de sécurité qui assume les fonctions nécessaires garantira que les données de sécurité et les informations de sécurité de l'organisation seront collectées, stockées, analysées, conservées et archivées ainsi que gérées, protégées et partagées comme prévu. Elle devrait spécifiquement identifier :

a) quelles données seront collectées ;

b) les définitions, la taxonomie et les formats des données ;

c) comment les données seront collectées, compilées et intégrées avec les autres sources de données de sécurité et d'informations de sécurité ;

d) comment les données de sécurité et les informations de sécurité seront stockées, archivées et sauvegardées ; par exemple, la structure de la base de données et, s'il y a un système de TI, l'architecture d'appui ;

e) comment les données de sécurité et les informations de sécurité seront utilisées ;

f) comment les informations devront être partagées et échangées avec d'autres parties ;

g) comment les données de sécurité et les informations de sécurité seront protégées selon le type et la source spécifiques des données de sécurité et des informations de sécurité ;

h) comment la qualité sera mesurée et maintenue.

5.5.3 En l'absence de processus clairement définis de production d'informations de sécurité, une organisation ne peut parvenir à fournir des informations défendables, fiables et cohérentes pouvant servir de base fiable à une prise de décisions fondées sur les données.

5.5.4 Gouvernance des données

La gouvernance des données désigne l'autorité, le contrôle et le pouvoir décisionnel sur les processus et procédures qui soutiennent les activités de gestion des données de l'organisation. Elle dicte comment les données de sécurité et les informations de sécurité sont collectées, analysées, utilisées, partagées et protégées. La gouvernance des données garantit que le ou les systèmes de gestion des données aient l'effet souhaité par le biais de caractéristiques clés d'intégrité, de disponibilité, de convivialité et de protection, comme indiqué ci-dessous.

Intégrité — L'intégrité des données désigne la fiabilité des sources, des renseignements et des événements qui y sont associés. Toutefois, l'intégrité des données inclut la maintenance et l'assurance de l'exactitude et de la cohérence des données sur tout leur cycle de vie. Il s'agit d'un aspect crucial de la conception, de la mise en œuvre et de l'usage du SDCPS pour le stockage, le traitement ou l'extraction des données.

Disponibilité — Il faut clairement indiquer qui est autorisé à utiliser ou à partager les données de sécurité et les informations de sécurité stockées. À cet égard, il convient de tenir compte de l'accord passé entre le propriétaire des données/informations et le dépositaire. Les entités autorisées à utiliser les données devraient savoir clairement comment accéder aux données et comment les traiter. Diverses techniques existent pour maximiser la disponibilité des données, y compris la redondance des lieux de stockage et les méthodes et outils d'accès aux données.

Convivialité — Pour maximiser le rendement des données de sécurité et des informations de sécurité, il importe d'étudier aussi les normes de convivialité. Les humains interagissent et travaillent sans cesse avec les données de sécurité et les informations de sécurité à mesure que celles-ci sont acquises. Les organisations devraient réduire au minimum les erreurs humaines par la mise en œuvre d'applications d'automatisation. Parmi les outils pouvant accroître la convivialité, citons les dictionnaires de données et les référentiels de métadonnées. À mesure que l'interaction humaine évolue vers des applications de mégadonnées et des processus d'apprentissage machine, il deviendra de plus en plus important de mieux comprendre la convivialité humaine telle qu'appliquée aux machines pour qu'à l'avenir, les erreurs de calcul dans les données de sécurité et les informations de sécurité soient réduites au minimum.

Protection — Les États devraient garantir que les données de sécurité, les informations de sécurité et les sources connexes bénéficient d'une protection appropriée. Voir le Chapitre 7 pour plus d'informations.

5.5.5 Gestion des métadonnées

5.5.5.1 On entend par métadonnées un ensemble de données qui décrit d'autres données et donne des informations au sujet de celles-ci, en d'autres termes des données sur des données. L'utilisation de normes de métadonnées donne une acception ou une définition commune de ces données. Elle assure une utilisation et une interprétation appropriées par les propriétaires et les utilisateurs et facilite l'extraction des données pour analyse.

5.5.5.2 Il importe que les organisations classent leurs données sur la base de leurs propriétés, en incluant, mais sans s'y limiter :

a) en quoi consistent les données ;

b) d'où elles proviennent (source originale) ;

c) qui les a créées ;

d) quand elles ont été créées ;

e) qui les a utilisées ;

f) à quelles fins elles ont été utilisées ;

g) la fréquence de collecte ;

h) tout traitement ou transformation.

5.5.5.3 Les métadonnées fournissent une compréhension commune de la nature des données et en garantissent un usage et une interprétation corrects par leurs propriétaires et utilisateurs. Elles permettent aussi d'identifier des erreurs dans la collecte de données, ce qui entraîne des améliorations continues du programme.

Chapitre 6

ANALYSE DE SÉCURITÉ

6.1 INTRODUCTION

6.1.1 L'analyse de sécurité est le processus qui consiste à appliquer des techniques statistiques ou d'autres techniques analytiques pour vérifier, examiner, décrire, transformer, condenser, évaluer et visualiser les données de sécurité et les informations de sécurité afin de découvrir des informations utiles, de suggérer des conclusions et de soutenir le processus décisionnel fondé sur les données. L'analyse aide les organisations à générer des informations de sécurité exploitables sous la forme de statistiques, de graphiques, de cartes, de tableaux de bord et d'exposés. L'analyse de sécurité est surtout précieuse pour de grandes organisations et/ou des organisations matures disposant d'une grande quantité de données de sécurité. Elle s'appuie sur l'application simultanée de recherches dans les domaines de la statistique, du calcul et de l'exploitation. Le résultat d'une analyse de sécurité devrait faire le point sur la sécurité dans des formats qui permettent aux décideurs de prendre des décisions fondées sur les données en matière de sécurité.

6.1.2 Les États sont tenus d'établir et de tenir à jour un processus destiné à analyser les données de sécurité et les informations de sécurité provenant du SDCPS et de bases de données de sécurité qui y sont liées. Un des objectifs de l'analyse des données de sécurité et des informations de sécurité au niveau de l'État est d'identifier les dangers systémiques et transversaux qui, sinon, pourraient ne pas être identifiés par les processus d'analyse des données de sécurité des différents prestataires de services.

6.1.3 L'analyse de sécurité peut être une nouvelle fonction que l'État ou le prestataire de services pourrait devoir créer. Il convient de noter que les compétences requises pour effectuer une analyse de sécurité efficace pourraient dépasser le cadre de compétences d'un inspecteur traditionnel de la sécurité. Les États et les prestataires de services devraient étudier les compétences nécessaires pour analyser les informations de sécurité et pour décider si, moyennant une formation appropriée, ce rôle devrait être une extension d'un poste existant ou s'il serait plus efficace de créer une nouvelle fonction, d'externaliser ce rôle ou d'utiliser une combinaison de ces approches. La décision sera fonction des plans et circonstances de chaque État ou prestataire de services.

6.1.4 Parallèlement aux considérations en matière de ressources humaines, il convient d'analyser le logiciel existant ainsi que les politiques et processus d'entreprise et de prise de décisions. Pour être efficace, l'analyse de sécurité devrait être intégrée dans les outils, politiques et processus fondamentaux existants de l'organisation. Une fois amalgamée, l'élaboration en continu de renseignements de sécurité devrait se faire sans heurts et devrait faire partie des pratiques d'entreprise habituelles de l'organisation.

6.1.5 L'analyse des données de sécurité et des informations de sécurité peut être effectuée de nombreuses manières, certaines exigeant des données et des capacités d'analyse plus solides que d'autres. L'utilisation d'outils adéquats pour l'analyse des données de sécurité et des informations de sécurité permet d'acquérir une compréhension plus précise de la situation générale en examinant les données sous des angles qui révèlent les relations, les connexions, les modèles et les tendances déjà présents en interne.

6.1.6 Une organisation ayant une capacité d'analyse mature est plus à même :

a) d'établir des métriques efficaces de la sécurité ;

b) d'établir des capacités de présentation de la sécurité (p. ex. tableau de bord de la sécurité) pour une interprétation aisée des informations de sécurité par les décideurs ;

c) d'assurer le suivi de la performance de sécurité d'un secteur, d'une organisation, d'un système ou d'un processus donné ;

d) de mettre en lumière les tendances et les cibles en matière de sécurité ;

e) d'alerter les décideurs sur la base de facteurs déclencheurs en matière de sécurité ;

f) d'identifier les facteurs de changement ;

g) d'identifier les connexions ou les « corrélations » entre ou parmi divers facteurs ;

h) de tester des hypothèses ;

i) de développer des capacités de modélisation prédictive.

6.1.7 Les organisations devraient inclure un éventail de sources d'informations appropriées dans leur analyse de sécurité, pas seulement des « données de sécurité ». Il est par exemple utile d'ajouter à l'ensemble de données des indications relatives, entre autres, à la météorologie, au relief, au trafic, à la démographie, à la géographie. Un accès à et une exploitation d'un éventail plus large de sources de données garantiront que les analystes et les décideurs en charge de la sécurité ont conscience du contexte plus général dans lequel les décisions en matière de sécurité sont prises.

6.1.8 Les États, en particulier, devraient s'intéresser tout spécialement aux informations qui identifient des tendances et des dangers en matière de sécurité qui transcendent tout le système aéronautique.

6.2 TYPES D'ANALYSE

L'analyse des données de sécurité et des informations de sécurité permet aussi aux décideurs de comparer les informations avec celles d'autres groupes (p. ex. un groupe de contrôle ou de comparaison) afin de permettre de tirer des conclusions des données de sécurité. Les approches courantes incluent l'analyse descriptive (décrire), l'analyse inférentielle (inférer) et l'analyse prédictive (prédire), comme illustré à la Figure 6-1.

6.2.1 Analyse descriptive

6.2.1.1 La statistique descriptive est utilisée pour décrire ou résumer les données sous des formes significatives et utiles. Elle permet de décrire, montrer ou résumer les données de façon que des modèles puissent émerger des données et elle contribue à définir clairement des études de cas, des possibilités et des défis. Les techniques descriptives fournissent des informations sur les données, mais elles ne permettent pas aux utilisateurs de tirer des conclusions au-delà des données analysées ou de dégager des conclusions sur toute hypothèse formulée à propos de ces données. Elles sont un moyen de décrire les données.

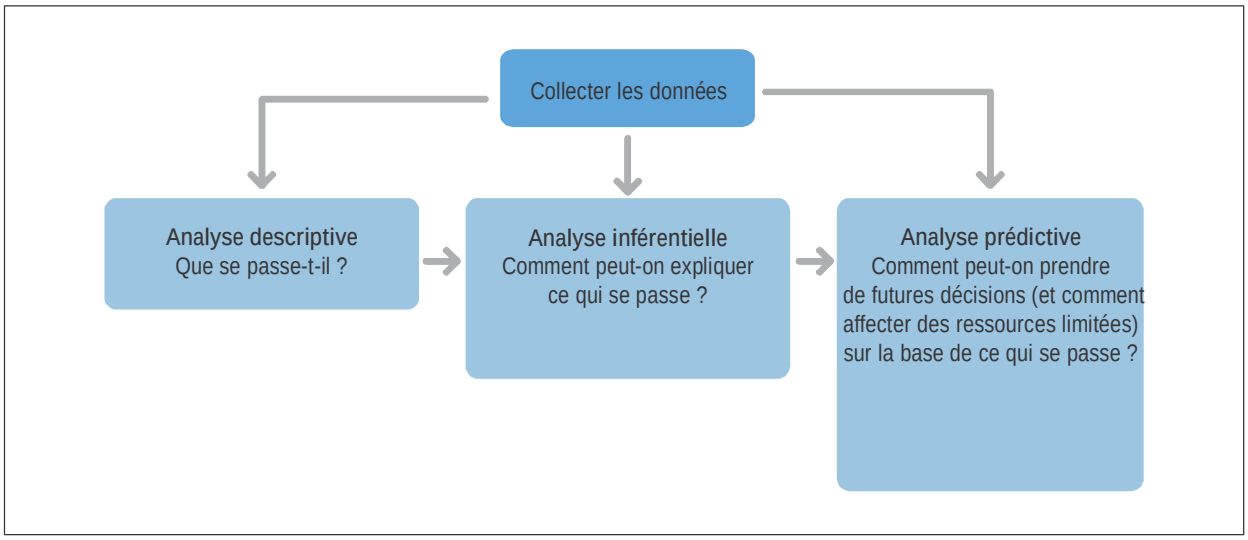

Figure 6-1. Types courants d'analyse statistique

6.2.1.2 La statistique descriptive est utile parce que si nous présentons uniquement les données brutes, en particulier en grandes quantités, il serait difficile de visualiser ce que les données nous montrent. La statistique descriptive permet aux utilisateurs de présenter et voir les données sous un angle plus intéressant, qui facilite l'interprétation des données. Tableaux et matrices, graphiques et diagrammes et même cartes sont autant d'exemples d'outils utilisés pour résumer les données. La statistique descriptive inclut des mesures de la tendance centrale, telles que la moyenne, la médiane et le mode, ainsi que des mesures de la variabilité telles que l'intervalle de variation, les quartiles, le minimum et le maximum, les distributions de fréquences, la variance et l'écart type (SD). Ces résumés peuvent soit constituer la base initiale pour décrire les données dans le cadre d'une analyse statistique plus vaste ou ils peuvent être suffisants en et pour eux-mêmes pour une investigation particulière.

6.2.2 Analyse inférentielle

La statistique inférentielle (ou inductive) vise à utiliser les données d'un échantillon pour tirer des conclusions sur la population que cet échantillon de données représente. Il n'est pas toujours commode ou possible d'examiner chaque individu d'une population entière et d'avoir accès à une population complète. Les statistiques inférentielles sont des techniques qui permettent aux utilisateurs des données disponibles de tirer des généralisations, des inférences et des conclusions sur la population dont des échantillons ont été pris aux fins de décrire des tendances. Elles comprennent des méthodes visant à estimer des paramètres, à vérifier des hypothèses statistiques, à comparer la performance moyenne de deux groupes sur la même mesure afin d'identifier des différences ou des similitudes, et à identifier d'éventuelles corrélations et relations entre variables.

6.2.3 Analyse prédictive

Il existe d'autres types d'analyse, notamment les analyses des probabilités ou analyses prédictives, qui extraient des informations des données historiques et actuelles et les utilisent pour prédire des tendances et des modèles de comportement. Les modèles trouvés dans les données permettent d'identifier les possibilités et les risques émergents. Souvent l'événement inconnu qui nous intéresse se situe dans l'avenir mais l'analyse prédictive peut être appliquée à n'importe quel type d'inconnue dans le passé, le présent ou l'avenir. Le cœur même de l'analyse prédictive repose sur la capture de relations entre des variables d'événements passés et sur l'exploitation de ces relations pour prédire le résultat inconnu. Certains systèmes permettent aux utilisateurs de modéliser différents scénarios de risques ou de

possibilités avec des résultats différents. Cela permet aux décideurs d'évaluer les décisions qu'ils peuvent prendre face à des circonstances inconnues différentes et de déterminer comment ils peuvent affecter avec efficacité des ressources limitées aux domaines où les possibilités ou les risques sont les plus grands.

6.2.4 Analyse combinée

6.2.4.1 Divers types d'analyses statistiques sont interconnectés et souvent effectués ensemble. Par exemple, une technique inférentielle peut être le principal outil utilisé pour tirer des conclusions sur un ensemble de données mais des statistiques descriptives sont aussi généralement utilisées et présentées. En outre, les extrants de statistiques inférentielles servent souvent de base à une analyse prédictive.

6.2.4.2 Des techniques analytiques peuvent être appliquées à l'analyse de sécurité pour :

a) identifier les causes et les facteurs contributifs liés aux dangers et aux éléments qui nuisent à l'amélioration continue de la sécurité de l'aviation ;

b) examiner les domaines dans lesquels l'efficacité des contrôles de sécurité peut être améliorée et renforcée ;

c) soutenir le suivi permanent de la performance et des tendances en matière de sécurité.

6.3 COMPTE RENDU DES RÉSULTATS DE L'ANALYSE

6.3.1 Les résultats de l'analyse des données de sécurité peuvent mettre en lumière les domaines à haut risque pour la sécurité et aider les décideurs et les cadres dirigeants à :

a) prendre des mesures correctrices immédiates ;

b) mettre en œuvre une surveillance fondée sur le risque de sécurité ;

c) définir ou affiner la politique de sécurité ou les objectifs de sécurité ;

d) définir ou affiner les SPI ;

e) définir ou affiner les SPT ;

f) établir des facteurs déclencheurs liés aux SPI ;

g) promouvoir la sécurité ;

h) mener d'autres évaluations des risques de sécurité.

6.3.2 Les résultats d'une analyse de sécurité devraient être mis à la disposition des parties intéressées par la sécurité de l'aviation dans un format facile à comprendre. Ces résultats devraient être présentés en gardant à l'esprit le public cible, à savoir les décideurs des organisations, les prestataires externes de services, les AAC et d'autres États. Les résultats d'une analyse de sécurité peuvent être présentés de plusieurs manières ; en voici quelques exemples :

a) Alertes de sécurité imminentes : pour communiquer à d'autres États ou prestataires de services des dangers pour la sécurité dont les résultats pourraient être catastrophiques et qui requièrent des mesures immédiates.

b) Rapports d'analyses de sécurité : présentent généralement des informations quantitatives et qualitatives, assorties d'une description claire du degré et de la source d'incertitude des constatations de l'analyse. Ces rapports peuvent aussi inclure des recommandations pertinentes concernant la sécurité.

c) Conférences sur la sécurité : pour permettre aux États et aux prestataires de services de partager des informations de sécurité et des résultats d'analyses de sécurité pouvant promouvoir des initiatives de collaboration.

6.3.3 Il est utile de traduire les recommandations en plans d'action, décisions et priorités que les décideurs de l'organisation doivent étudier et, si possible, d'indiquer qui doit faire quoi des résultats de l'analyse et pour quand.

6.3.4 Des outils de visualisation tels que diagrammes, graphiques, images et tableaux de bord sont des moyens simples mais efficaces de présenter les résultats de l'analyse des données. Plusieurs exemples de rapports visuels d'analyse des données sont disponibles dans le système intégré d'analyse et de compte rendu des tendances de la sécurité (iSTARS) de l'OACI, sur la page https://icao.int/safety/iSTARS.

6.3.5 Tableaux de bord de la sécurité

6.3.5.1 La performance de sécurité de l'organisation devrait être démontrable et devrait clairement indiquer à toutes les parties intéressées que la sécurité est gérée efficacement. Une manière de le prouver est d'utiliser un « tableau de bord de la sécurité », à savoir une représentation visuelle qui offre aux cadres supérieurs, aux gestionnaires et aux professionnels de la sécurité un moyen rapide et aisé de visualiser la performance de sécurité de l'organisation.

6.3.5.2 En plus de la visualisation en temps réel des SPI et SPT de l'organisation, les tableaux de bord peuvent aussi inclure des informations sur la catégorie, la cause et la gravité de dangers spécifiques. Idéalement, les informations présentées sur le tableau de bord peuvent être personnalisées pour afficher les informations nécessaires au processus décisionnel à différents niveaux de l'organisation. L'utilisation de facteurs déclencheurs est utile pour fournir des aides visuelles de base afin de mettre en lumière les éventuels problèmes à résoudre pour un indicateur spécifique. Les analystes et les décideurs voudront avoir la possibilité de configurer le tableau de bord pour afficher leurs indicateurs principaux ainsi qu'une caractéristique qui leur permet d'approfondir les métriques.

6.3.5.3 La collecte et l'analyse des données nécessaires pour une prise de décisions et une gestion efficaces doivent se faire en continu. Les résultats de l'analyse des données peuvent révéler qu'il faut accroître la quantité et améliorer la qualité des données collectées et analysées pour appuyer les mesures et décisions que l'organisation doit prendre. La Figure 6-2 montre comment le compte rendu des résultats de l'analyse peut déterminer si des données complémentaires doivent être collectées.

6.4 PARTAGE ET ÉCHANGE DES INFORMATIONS DE SÉCURITÉ

La sécurité peut encore être améliorée par le partage et l'échange d'informations de sécurité. De tels partages et échanges garantissent une réaction cohérente, transparente et fondée sur les données à des préoccupations de sécurité aux niveaux mondial, national et organisationnel. Le partage d'informations de sécurité désigne le fait de donner de telles informations, tandis que l'échange couvre l'action de donner et de recevoir en retour.

6.4.1 Partager au sein de l'État

6.4.1.1 Il est recommandé que chaque État encourage l'établissement de réseaux pour le partage ou l'échange d'informations de sécurité entre les usagers du système aéronautique et facilite le partage et l'échange d'informations de sécurité, sauf si le droit national s'y oppose. Des orientations sur la promotion de la sécurité à l'attention des États et des prestataires de services sont données aux Chapitres 8 et 9, respectivement.

6.4.1.2 Le niveau de protection et les conditions auxquelles des informations de sécurité seront partagées ou échangées entre autorités de l'État et prestataires de services doivent être conformes aux législations nationales. De plus amples informations sur la protection des données de sécurité et des informations de sécurité figurent au Chapitre 7.

6.4.2 Partager entre États

Si, en analysant les informations que contient son SDCPS, un État trouve des éléments touchant la sécurité qui peuvent intéresser d'autres États, il est recommandé qu'il les communique à ceux-ci dès que possible. Les États sont aussi encouragés à partager les informations de sécurité au sein de leur RASG. Avant de partager des informations de sécurité, les États devraient s'assurer que le niveau de protection et les conditions auxquelles les informations de sécurité seront partagées sont conformes aux dispositions de l'Annexe 19, Appendice 3. Des éléments indicatifs détaillés sont disponibles au Chapitre 7.

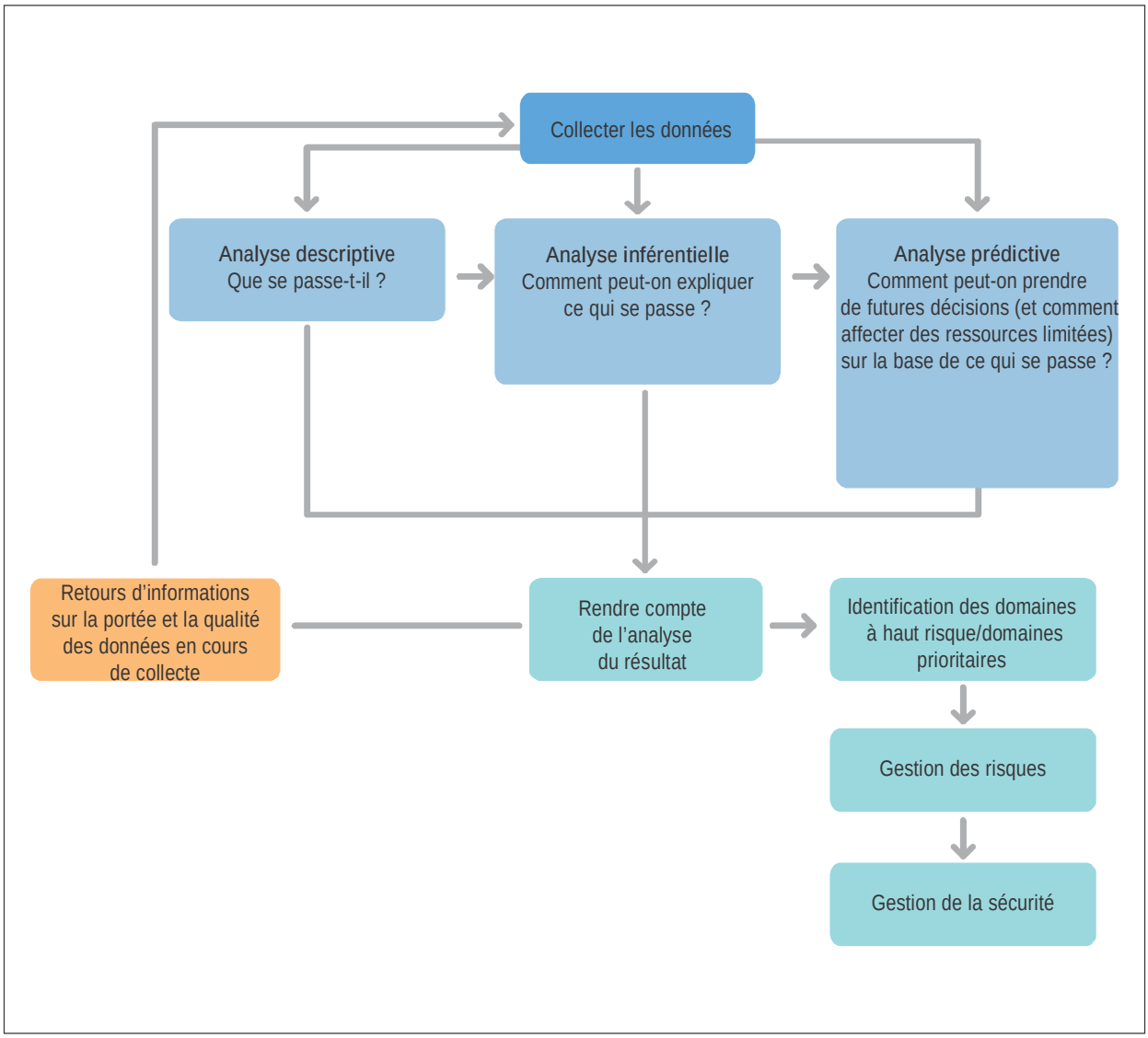

Figure 6-2. Intégration du processus décisionnel fondé sur les données dans la gestion de la sécurité

6.5 PROCESSUS DÉCISIONNEL FONDÉ SUR LES DONNÉES

6.5.1 Le but premier de l'analyse de sécurité et des comptes rendus de sécurité est de présenter aux décideurs un point sur la sécurité qui leur permettra de prendre des décisions fondées sur les données présentées. On parle dans ce cas de processus décisionnel fondé sur les données (aussi appelé PDFD ou D3M), soit une approche de la prise de décisions axée sur les processus.

6.5.2 Beaucoup d'événements en aviation sont le résultat, tout au moins en partie, de mauvaises décisions de gestion, qui peuvent entraîner du gaspillage d'argent, de main-d'œuvre et de ressources. Le but des décideurs en charge de la sécurité est, à court terme, de réduire au minimum les mauvais résultats et d'atteindre des résultats positifs effectifs et, à long terme, de contribuer à la réalisation des objectifs de l'organisation en matière de sécurité.

6.5.3 Une bonne prise de décisions n'est pas un processus facile. Des décisions sont souvent prises sans possibilité de prendre en considération tous les facteurs pertinents. Les décideurs sont aussi susceptibles de biais qui, consciemment ou non, affectent les décisions prises.

6.5.4 Le but du PDFD n'est pas nécessairement la prise de la décision « parfaite » ou idéale mais plutôt la prise d'une bonne décision qui permettra de réaliser l'objectif à court terme (en vue duquel la décision réelle est prise) et œuvrera à la satisfaction de l'objectif à long terme (améliorer la performance de sécurité de l'organisation). De bonnes décisions répondent aux critères suivants :

a) *Transparence :* la communauté aéronautique devrait connaître tous les facteurs qui influencent une décision, y compris le processus suivi pour parvenir à cette décision.

b) *Responsabilité :* la décision et les résultats qui en découlent « appartiennent » au décideur. Clarté et transparence induisent aussi une responsabilité — il n'est pas facile de se cacher derrière une décision pour laquelle les rôles et responsabilités sont définis en détail et les attentes liées à la nouvelle décision sont clairement précisées.

c) *Équité et objectivité :* le décideur n'est pas influencé par des considérations non pertinentes (p. ex. des avantages financiers ou des relations personnelles).

d) *Justifiabilité et défendabilité :* il est possible de prouver que la décision est raisonnable vu les éléments sur la base desquels la décision repose et vu le processus suivi.

e) *Reproductibilité :* confrontée à des informations identiques à celles dont disposait le décideur et en suivant le même processus, une autre personne arriverait à la même décision.

f) *Exécutabilité :* la décision est suffisamment claire et cette clarté réduit au minimum l'incertitude.

g) *Pragmatisme :* les humains sont des créatures d'émotion, ce qui signifie qu'il n'est pas possible d'éliminer l'émotion d'une décision. Toutefois, ce que l'on peut éliminer, ce sont les biais émotionnels intéressés. Face à une décision difficile, il est sain de poser la question suivante : à qui profite la décision ?

6.5.5 Avantages d'un processus décisionnel fondé sur les données

6.5.5.1 Le PDFD permet aux décideurs de se concentrer sur les résultats de sécurité souhaités, qui sont cohérents avec la politique de sécurité et avec les objectifs de sécurité, et de tenir compte de divers aspects liés à la gestion du changement, aux évaluations des risques de sécurité, etc. Le PDFD peut aider à la prise de décisions relatives :

a) aux changements prévisibles dans les exigences statutaires et réglementaires, les technologies émergentes ou les ressources et susceptibles d'affecter l'organisation ;

b) aux changements potentiels des besoins et attentes de la communauté aéronautique et des parties intéressées ;

c) aux diverses priorités qu'il faut établir et gérer (p. ex. stratégiques, opérationnelles, relatives aux ressources) ;

d) aux nouvelles aptitudes, compétences, aux nouveaux outils et même aux processus de gestion du changement qui peuvent se révéler nécessaires pour mettre en œuvre une ou plusieurs nouvelles décisions ;

e) aux risques qu'il faut évaluer, gérer ou atténuer ;

f) aux services, produits et processus existants qui sont les plus rentables pour les parties intéressées ;

g) à l'évolution des demandes de nouveaux services, produits et processus.

6.5.5.2 Une approche structurée telle que le PDFD mène les décideurs à prendre des décisions alignées sur ce qu'indiquent les données de sécurité. Pour cela, il faut avoir confiance dans le cadre de gestion de la performance de sécurité ; si les personnes ont confiance dans le SDCPS, elles auront confiance dans toute décision qui en découle.

6.5.6 Défis courants posés par le processus décisionnel fondé sur les données

6.5.6.1 La mise en œuvre de processus de collecte et d'analyse de données demande du temps et de l'argent, ainsi que des savoir-faire et des compétences qui ne seront pas nécessairement disponibles dans l'organisation. Il faut étudier en détail le temps et les ressources que requiert le processus décisionnel. Les facteurs à prendre en considération incluent la somme d'argent associée à la décision, la portée de la décision et la permanence de l'effet de cette décision sur la sécurité. Si l'organisation ne comprend pas les enjeux, le PDFD peut devenir une source de frustration pour les décideurs en charge de la sécurité, qui pourraient dès lors saper ou abandonner le processus. Tout comme le PNS et le SGS, le PDFD et la gestion de la performance de sécurité exigent un engagement à créer et maintenir les structures et compétences nécessaires pour maximiser les possibilités offertes par le PDFD.

6.5.6.2 Il est plus difficile de générer la confiance dans des données que de faire confiance à la contribution et à l'avis d'un expert. L'adoption de l'approche PDFD exige un changement de culture et d'état d'esprit de l'organisation pour passer à un modèle où les décisions reposent sur des SPI fiables et sur les résultats de l'analyse d'autres données de sécurité.

6.5.6.3 Dans certains cas, le processus décisionnel peut s'enliser dans une tentative de trouver la « meilleure solution possible » ; on parle alors de « paralysie de l'analyse ». Des stratégies peuvent être utilisées pour éviter cela :

a) fixer une date limite ;

b) avoir une portée et un objectif clairement définis ;

c) ne pas viser une décision ou une solution « parfaite » du premier coup, mais plutôt parvenir à une décision « appropriée » et « pratique » et améliorer les décisions ultérieures.

6.5.7 Processus décisionnel fondé sur les données

6.5.7.1 Le PDFD peut être un outil crucial qui accroît la valeur et l'efficacité du PNS et du SGS. Une gestion efficace de la sécurité dépend de la prise de décisions défendables, en connaissance de cause. Un PDFD efficace s'appuie, à son tour, sur des besoins clairement définis de données de sécurité et d'informations de sécurité, ainsi que sur des normes, des méthodes de collecte, une gestion des données, l'analyse et le partage de données, qui sont autant de composantes du PDFD. La Figure 6-3 illustre le PDFD.

Étape 1 — Définir le problème ou l'objectif

6.5.7.2 La première étape de la planification et de la mise en place d'un PDFD consiste à définir le problème à résoudre ou l'objectif de sécurité à atteindre. À quelle question faut-il répondre ? Quelle décision les décideurs doivent-ils prendre en matière de sécurité ? Comment cette décision s'intégrera-t-elle dans les objectifs organisationnels plus stratégiques ? Au cours du processus de définition du problème, les décideurs devraient se poser les questions suivantes :

a) La collecte et l'analyse des données soutiennent-elles les objectifs de sécurité ou les cibles de sécurité de l'organisation et y sont-elles liées ?

b) Les données requises sont-elles disponibles ? Ou peuvent-elles être obtenues d'une manière raisonnable ?

c) Est-il commode et possible de collecter et analyser les données ?

d) Les ressources requises (personnel, équipement, logiciel, fonds) sont-elles disponibles ?

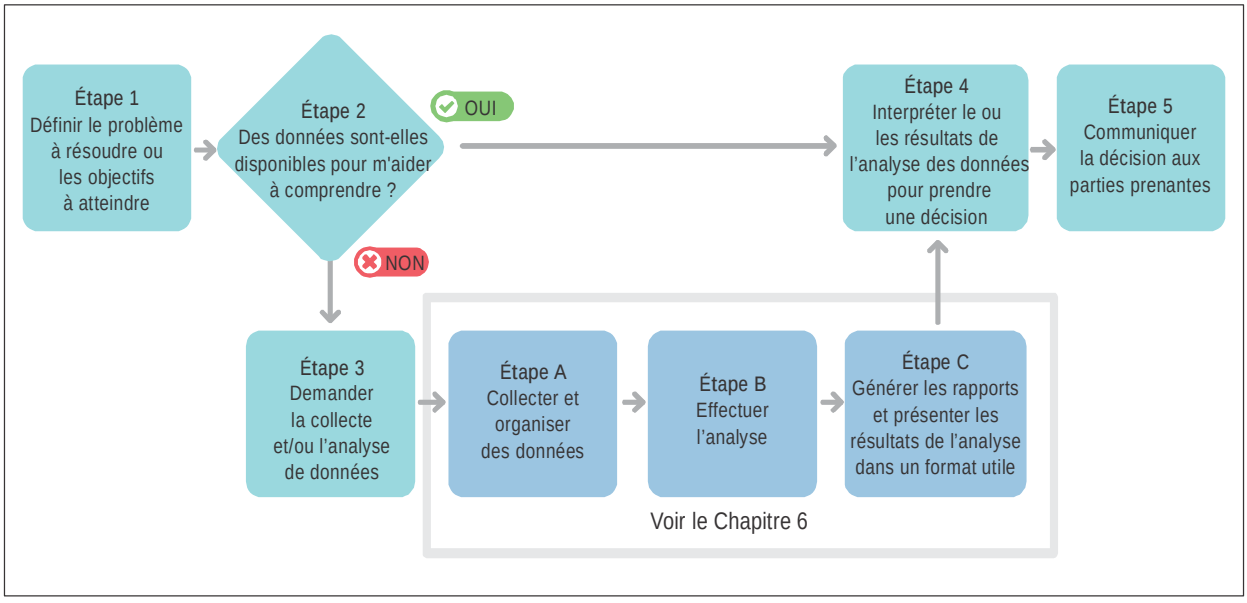

Figure 6-3. Étapes du processus décisionnel fondé sur les données

6.5.7.3 Dans le contexte de la gestion de la sécurité, les principaux énoncés de problèmes au sein de l'organisation concernent l'évaluation et la sélection des priorités de sécurité — en conformité avec les objectifs de sécurité — et la mise en place de mesures d'atténuation des risques de sécurité.

Étape 2 — Accéder à des données pour soutenir le processus décisionnel

6.5.7.4 L'étape suivante consiste à identifier les données requises pour résoudre le problème (en tenant compte des dispositions sur la protection des informations). Aucune donnée n'est plus intéressante qu'une autre. Il faudrait s'attacher à déterminer si les données disponibles sont appropriées pour contribuer à répondre à la question et à résoudre le problème. Si les données requises sont disponibles, passer à l'étape 4. Si les données adéquates ne sont pas disponibles, l'organisation devra collecter, stocker, analyser et présenter les nouvelles données de sécurité et les nouvelles informations de sécurité de façons utiles.

Étape 3 — Demander des données pour soutenir le processus décisionnel

6.5.7.5 Si les données ne sont pas déjà disponibles, l'organisation doit trouver des moyens de les collecter. Pour ce faire, elle devra peut-être établir un autre SPI et, éventuellement, des SPT alignées. L'établissement d'indicateurs supplémentaires peut être coûteux. Une fois le coût connu, l'organisation devrait estimer si les avantages compensent ce coût. Il faudrait s'attacher surtout à identifier, suivre et mesurer les données de sécurité requises pour prendre des décisions efficaces fondées sur les données en matière de sécurité. Si le coût est supérieur aux avantages, envisager d'autres sources de données et/ou indicateurs.

6.5.7.6 Dans l'étape de planification du PDFD, l'organisation doit définir ce qu'elle veut atteindre en établissant des SPT et des SPI et en analysant les données. Pourquoi l'organisation doit-elle résoudre le problème identifié ? Qu'est-ce qu'une cible raisonnable ? Comment et où les responsables de la sécurité utiliseront-ils les résultats de la collecte et de l'analyse des données ? Pour tout SDCPS, il est fondamental d'avoir une idée claire des raisons pour lesquelles l'organisation doit collecter, analyser, partager et échanger des données de sécurité et des informations de sécurité.

6.5.7.7 Les éléments suivants se combinent pour permettre à l'organisation d'identifier des tendances, de prendre des décisions en connaissance de cause, d'évaluer la performance de sécurité par rapport aux objectifs définis, d'évaluer les risques ou de répondre à ses besoins :

a) la gestion de la performance de sécurité — en tant que cadre de gouvernance des données de sécurité et des informations de sécurité ;

b) le SDCPS — en tant que fonctionnalité de collecte et de traitement des données de sécurité ;

c) le PDFD — en tant que processus décisionnel fiable.

Étape 4 — Interpréter les résultats de l'analyse des données et prendre une décision fondée sur les données

6.5.7.8 Les données collectées doivent être présentées aux décideurs au bon moment et dans des formats utiles. La pertinence et la taille des ensembles de données, la sophistication de l'analytique et les compétences des analystes des données ne seront efficaces que si les données sont présentées quand elles sont nécessaires et dans des formats faciles à appréhender par les décideurs. Les éclairages tirés de ces données devraient alimenter le processus décisionnel et, à terme, améliorer la performance de sécurité.

6.5.7.9 Il existe de nombreux modèles de prise de décision. L'utilisation d'une approche normalisée et convenue maximisera la cohérence et l'efficacité des décisions fondées sur les données prises par l'organisation. La plupart comportent les étapes suivantes :

a) réunir une équipe/un groupe ayant les compétences et l'expérience nécessaires (p. ex. groupe d'action pour la sécurité [SAG]) ;

b) définir clairement le problème ou l'objectif de sécurité et le contexte ;

c) analyser les SPT et les objectifs de sécurité de l'organisation pour veiller à ce qu'ils restent alignés ;

d) analyser et interpréter les données de sécurité pour comprendre ce qu'elles indiquent ;

e) envisager et analyser les alternatives viables ;

f) envisager le risque lié aux actions faisables (ou inactions) ;

g) dégager un consensus au sein du groupe de prise de décisions ;

h) s'engager en faveur de la décision fondée sur les données et l'appliquer (transformer les données en action) ;

i) suivre et évaluer les résultats.

Étape 5 — Communiquer la décision

6.5.7.10 Pour que la décision de sécurité soit efficace, elle doit être communiquée aux parties prenantes, notamment :

a) au personnel qui doit appliquer les mesures nécessaires ;

b) à la personne qui a signalé la situation (si nécessaire) ;

c) à tout le personnel, pour s'assurer qu'il soit tenu au courant des améliorations de la sécurité (promotion de la sécurité : pour les États, voir le Chapitre 8 ; pour les prestataires de services, voir le Chapitre 9) ;

d) aux gestionnaires des connaissances de l'organisation pour s'assurer que la décision de sécurité est intégrée dans l'apprentissage de l'organisation.

6.5.7.11 Pour plus d'informations sur les communications relatives à la sécurité, voir les § 8.6, pour les États, et 9.6, pour les prestataires de services.

Chapitre 7

PROTECTION DES DONNÉES DE SÉCURITÉ, DES INFORMATIONS DE SÉCURITÉ ET DES SOURCES CONNEXES

7.1 OBJECTIFS ET CONTENU

7.1.1 Le présent chapitre décrit les principes fondamentaux régissant la protection des données de sécurité et des informations de sécurité saisies par des systèmes de compte rendu de sécurité ou tirées de tels systèmes, ainsi que des sources de telles données et informations[1]. Il donne en outre des orientations et conseils sur la mise en œuvre de ces principes par les autorités de réglementation de l'aviation, les prestataires de services, les législateurs, les juristes, les procureurs, les fonctionnaires judiciaires et autres autorités compétentes de l'État chargés de prendre des décisions sur l'utilisation et la protection des données de sécurité, des informations de sécurité et de leurs sources connexes. Le présent chapitre peut être utile pour toute autre personne souhaitant accéder à des données de sécurité ou à des informations de sécurité, ou souhaitant divulguer ces données ou informations.

7.1.2 Le présent chapitre aborde les sujets suivants :

a) principes fondamentaux ;

b) portée de la protection et niveau de protection ;

c) principes régissant la protection ;

d) principes régissant les dérogations ;

e) divulgation au public ;

f) protection des données enregistrées ;

g) partage et échange des informations de sécurité.

7.2 PRINCIPES FONDAMENTAUX

7.2.1 La protection des données de sécurité, des informations de sécurité et de leurs sources connexes vise à garantir leur disponibilité en continu, afin qu'elles puissent être utilisées pour maintenir ou améliorer la sécurité de l'aviation, tout en encourageant les individus et les organisations à rendre compte des données de sécurité et des informations de sécurité. Dans ce contexte, on ne soulignera jamais assez l'importance de mettre en place des protections. Les protections n'entendent pas exonérer les sources de leurs obligations en matière de sécurité ou entraver l'administration appropriée de la justice.

1. Conformément à l'Annexe 19, les sources des données de sécurité et des informations de sécurité incluent tant des individus que des organisations.

7.2.2 La sécurité de l'aviation n'est pas de la seule responsabilité des États ou des prestataires de services. C'est une responsabilité partagée, à laquelle toutes les parties prenantes devraient contribuer en fournissant, entre autres, des données et informations pertinentes par le biais de comptes rendus en matière de sécurité.

7.2.3 Alors que les données et informations peuvent provenir de diverses sources, la communication de données de sécurité et d'informations de sécurité par des individus et des organisations du système aéronautique est un élément fondamental de la gestion de la sécurité. Des systèmes efficaces de compte rendu en matière de sécurité contribuent à garantir que les personnes sont et restent disposées à rendre compte de leurs erreurs et expériences afin que les États et les prestataires de services aient accès aux données et informations pertinentes qui sont nécessaires pour remédier aux carences et aux dangers de sécurité existants et potentiels. Cette garantie est fournie par la création d'un environnement dans lequel les personnes peuvent avoir la certitude que les données de sécurité et les informations de sécurité seront utilisées exclusivement pour maintenir et améliorer la sécurité, à moins qu'un des principes régissant les dérogations ne s'applique.

7.2.4 L'Annexe 19 ne prévoit pas de protection pour les individus ou organisations mentionnés dans le compte rendu. Toutefois, les États peuvent étendre la protection aux individus ou organisations mentionnés dans le compte rendu.

7.2.5 Il est important que tant les individus que les organisations soient protégés, de même que les données de sécurité et les informations de sécurité dont ils rendent compte. Pour protéger les individus et organisations, il faut :

a) s'assurer qu'ils ne soient pas punis sur la base de leur compte rendu ;

b) limiter l'utilisation des données de sécurité et des informations de sécurité figurant dans le compte rendu à des finalités visant à maintenir ou à améliorer la sécurité.

Ces protections s'appliquent sauf si un des principes régissant les dérogations énoncés ci-dessous s'applique.

7.2.6 L'Annexe 19 exige que les États veillent à ce que les données de sécurité et les informations de sécurité ne soient pas utilisées à d'autres fins que celles qui sont exposées dans les ***principes régissant la protection,*** sauf si un des principes régissant les dérogations s'applique. Les ***principes régissant les dérogations*** exposent les circonstances dans lesquelles une dérogation à ces principes de protection peut être accordée.

7.2.7 Des mesures de prévention, de correction ou de remédiation, basées sur les données de sécurité et les informations de sécurité communiquées, peuvent, si nécessaire, être prises par les États et les prestataires de services aux fins de maintenir ou d'améliorer la sécurité — c'est-à-dire pour permettre aux États et aux prestataires de services de prendre des mesures appropriées pour :

a) se protéger contre la possibilité qu'un risque de sécurité cause dans l'immédiat un préjudice ou des blessures, jusqu'à ce que ce risque puisse être identifié et atténué ;

b) veiller à ce que des mesures appropriées soient prises pour réduire au minimum la probabilité qu'un tel risque puisse se reproduire à l'avenir ;

c) prévenir une exposition à un risque de sécurité non atténué ;

d) garantir l'intégrité du système de compte rendu lui-même et du système plus vaste dont il fait partie.

7.2.8 Comme de telles mesures sont fondamentales pour atteindre les objectifs et l'efficacité de tout système de gestion de la sécurité, l'Annexe 19 stipule expressément qu'il ne sera pas interdit aux États de prendre des mesures de prévention, de correction ou de remédiation pour maintenir ou améliorer la sécurité de l'aviation. De telles mesures peuvent être prises dans le cadre des processus applicables de gestion de la sécurité et ne sont donc pas soumises aux principes régissant les dérogations énoncés dans l'Annexe 19.

7.2.9 Des mesures de prévention, de correction ou de remédiation peuvent amener à restreindre, limiter ou empêcher[2] l'exercice de certains privilèges[3], la prestation de services ou l'exploitation d'un aéronef, jusqu'à ce que les risques de sécurité identifiés aient été résolus efficacement. Lorsqu'elles sont prises à de telles fins, en vertu de protocoles établis, les mesures de protection ou de précaution ne doivent pas être considérées comme punitives ou disciplinaires. Le but de telles mesures est d'empêcher ou de réduire au minimum l'exposition à un risque de sécurité non atténué.

7.2.10 Les principes liés à la protection des données de sécurité et des informations de sécurité et de leurs sources, contenus dans l'Annexe 19, prévoient une clarté et une transparence accrues, ainsi qu'un terrain de jeu égal, en vue de faciliter l'échange de données de sécurité et d'informations de sécurité entre États, comme l'exige l'Annexe 19.

7.3 PORTÉE DE LA PROTECTION

7.3.1 Étendue des données de sécurité et des informations de sécurité couvertes par les principes de protection

7.3.1.1 La protection s'applique aux données de sécurité saisies par des systèmes de compte rendu volontaire en matière de sécurité et par des sources connexes et aux informations de sécurité tirées de ces systèmes et sources. Ce principe peut s'appliquer à des systèmes de compte rendu obligatoire en matière de sécurité, là où de tels systèmes sont en vigueur (voir § 7.4.3 ci-dessous). Les sources de données de sécurité et d'informations de sécurité peuvent être des individus ou des organisations.

7.3.1.2 Dans certains États, les systèmes de compte rendu de sécurité peuvent couvrir les données communiquées à des enquêtes de sécurité menées par les autorités de l'État ou par des prestataires de services aéronautiques, les données et informations saisies par des systèmes de compte rendu par autodivulgation (y compris les systèmes de saisie automatique de données et les systèmes de saisie manuelle de données) ou d'autres données et informations de sécurité pertinentes. Les principes régissant la protection et les dérogations peuvent dès lors être étendus aux données de sécurité et aux informations de sécurité saisies par ces systèmes.

7.3.1.3 Les principes régissant la protection et les dérogations s'appliquent aussi à d'autres cas. Par exemple, l'Annexe 6 — *Exploitation technique des aéronefs,* Partie 1 — *Aviation de transport commercial international — Avions*, stipule que les sources des programmes d'analyse des données de vol (FDA) devraient être protégées conformément aux principes énoncés dans l'Annexe 19.

7.3.1.4 Le type de données de sécurité et d'informations de sécurité qui peuvent être saisies par des systèmes de compte rendu en matière de sécurité et les types de systèmes qui peuvent faire partie de tels systèmes peuvent évoluer au fil du temps, parallèlement à l'évolution des systèmes de gestion de la sécurité eux-mêmes. Les données de sécurité, les informations de sécurité et les systèmes de compte rendu en matière de sécurité qui ne sont pas expressément identifiés dans l'Annexe 19 aujourd'hui pourraient être régis par l'Annexe 19 à l'avenir.

7.3.2 Interaction avec les principes de protection contenus dans d'autres Annexes

7.3.2.1 Certains types de données de sécurité et d'informations de sécurité qui sont protégés en vertu de l'Annexe 19 peuvent, dans certaines circonstances, être soumis à d'autres exigences de protection.

2. Pour empêcher l'exercice de privilèges, on peut notamment suspendre ou révoquer des privilèges liés à une licence.
3. Les privilèges d'un titulaire d'autorisation sont spécifiés par la licence ou le certificat délivré par les autorités nationales de réglementation de l'aviation.

7.3.2.2 En particulier, l'Annexe 19 spécifie que lorsqu'une enquête est instituée conformément à l'Annexe 13, les éléments d'enquête sur les accidents et les incidents énumérés à l'Annexe 13 feront l'objet des protections prévues à l'Annexe 13 et non des protections prévues dans l'Annexe 19.

7.3.2.3 Ce principe s'applique à partir du moment où un accident ou un incident au sens de l'Annexe 13 se produit et reste d'application même après la publication du rapport final. Des orientations sur la protection des éléments d'enquête sur les accidents et les incidents sont fournies dans le *Manuel relatif à la protection des informations sur la sécurité* (Doc 10053).

7.3.2.4 De même, alors que l'Annexe 19 prévoit une protection pour les données enregistrées lorsque celles-ci sont utilisées à des fins de gestion de la sécurité, l'Annexe 6 accorde une protection aux enregistrements des enregistreurs de bord en opérations normales, en dehors des enquêtes du type de l'Annexe 13.

7.3.2.5 L'Annexe 6 aborde l'utilisation des enregistreurs de conversations de poste de pilotage (CVR) et des enregistreurs d'images embarqués (AIR), qui devrait se limiter à des fins liées à la sécurité et s'accompagner de sauvegardes appropriées, pour les inspections des enregistreurs de bord ou en cas de recherche d'enregistrements ou de transcriptions connexes dans le cadre de procédures pénales. Ces procédures pénales sont prises en compte dans l'amendement en tant que dérogation aux mesures de protection prévues pour les CVR et les AIR, afin de permettre aux autorités compétentes d'accéder sans restriction à ces types d'enregistrements et à leurs transcriptions et d'utiliser ceux-ci sans restriction lorsque des infractions pénales ont été commises et que les membres d'équipage impliqués n'ont peut-être pas consenti à l'utilisation de ces enregistrements et transcriptions (actes de piraterie aérienne, par exemple).

7.3.2.6 De même, les enregistreurs de données de vol (FDR), les systèmes d'enregistrement de données d'aéronef (ADRS) ainsi que les enregistreurs AIR de classes B et C, et les systèmes d'enregistrement d'images embarqués (AIRS) ne devraient être utilisés qu'à des fins de navigabilité ou de maintenance, notamment pour les programmes d'analyse des données de vol, avec les protections adéquates accordées par l'Annexe 19.

7.3.2.7 La Figure 7-1 donne des orientations générales concernant l'interaction entre les cadres de protection des Annexes 6, 13 et 19 et est à utiliser en consultation avec les dispositions applicables.

7.3.2.8 En ce qui concerne les programmes FDA, les sources restent, dans toute situation, protégées par les principes contenus dans l'Annexe 19.

7.3.3 Application des principes de l'Annexe 19 aux prestataires de services

7.3.3.1 L'Annexe 19 décrit un environnement de compte rendu qui favorise la confiance comme un environnement « dans lequel les employés et le personnel d'exploitation peuvent avoir confiance qu'ils ne seront pas sanctionnés pour des actions ou omissions qui correspondent à leur formation et leur expérience ». Une action ou omission est proportionnelle à la formation et à l'expérience d'une personne lorsqu'il est raisonnable de s'attendre à ce qu'une personne du même niveau d'expérience et de formation puisse faire, ou omettre de faire, la même chose. Un tel environnement est indispensable pour obtenir des comptes rendus en matière de sécurité efficaces et efficients.

7.3.3.2 Pour encourager les individus à rendre compte de données de sécurité ou d'informations de sécurité pertinentes, il faut que les sources de ces comptes rendus soient protégées contre des mesures prises par les États conformément à l'Annexe 19, ainsi que contre des mesures prises au sein de leur environnement de travail.

7.3.3.3 Les dispositions des Annexes sont conçues pour prévoir les exigences minimales auxquelles tous les États doivent satisfaire, quelles que soient l'ampleur et la complexité de leurs activités d'aviation civile. Il incombe à chaque État d'élaborer des exigences suffisantes pour assurer une conformité satisfaisante de l'État et de ses prestataires de services.

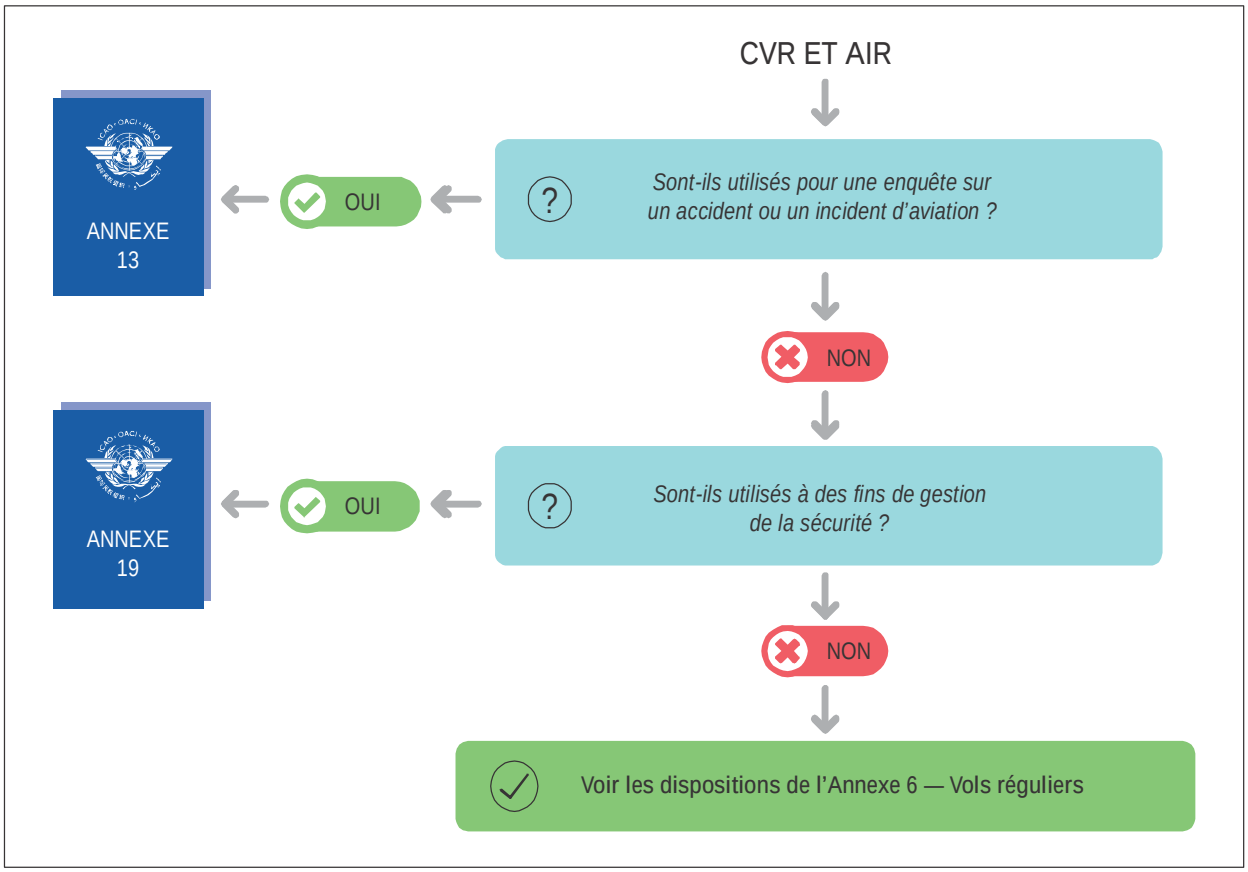

Figure 7-1. Orientations sur l'interaction entre dispositions de protection

7.3.3.4 Les principes régissant la protection et les dérogations qui s'appliquent aux données de sécurité, aux informations de sécurité et aux sources connexes en vertu de l'Annexe 19 devraient être mis en œuvre tant par les États que par les prestataires de services. Pour garantir la réalisation de cet objectif, les États doivent adopter des lois, des réglementations et des politiques nationales pertinentes, afin de s'assurer que leurs prestataires de services appliquent les dispositions contenues dans l'Annexe 19.

7.4 NIVEAU DE PROTECTION

7.4.1 Conditions pour bénéficier de la protection prévue à l'Annexe 19

7.4.1.1 L'Annexe 19 exige que les États déterminent les conditions auxquelles les données de sécurité et les informations de sécurité peuvent être protégées. Pour ce faire, les États doivent étudier :

a) si les données de sécurité ou les informations de sécurité sont couvertes par l'Annexe 19 ;

b) s'il existe des circonstances dans lesquelles l'Annexe 6 ou l'Annexe 13 primerait sur l'Annexe 19 ;

c) si un des principes régissant les dérogations s'applique.

7.4.2 Actions nécessaires pour maintenir ou améliorer la sécurité de l'aviation

7.4.2.1 L'Annexe 19 garantit que les États et les prestataires de services ne soient pas empêchés d'utiliser des données de sécurité ou des informations de sécurité pour prendre des mesures de prévention, de correction ou de remédiation nécessaires au maintien ou à l'amélioration de la sécurité de l'aviation. Conformément à cet objectif, il faudrait éviter, dans la mesure du possible, qu'une telle mesure, si elle était prise, ait une incidence néfaste sur les finances, la réputation ou tout autre aspect de la source desdites données de sécurité ou informations de sécurité.

7.4.2.2 Des mesures de prévention, de correction ou de remédiation visent à tenir compte des circonstances ou conditions qui posent des risques inacceptables pour la sécurité de l'aviation.

7.4.2.3 Une *mesure de prévention* peut être comprise comme une mesure prise pour prévenir l'occurrence ou la récurrence d'un événement ou d'un danger qui pose un risque pour la sécurité.

7.4.2.4 Une *mesure de correction* peut être comprise comme une mesure prise pour remédier à des lacunes ou à des carences particulières liées à la sécurité, notamment en cas d'incapacité d'un titulaire d'autorisation de prouver sa conformité aux normes applicables en matière de sécurité ou de compétences. Des mesures de correction peuvent être nécessaires pour restaurer la conformité d'un titulaire d'autorisation.

7.4.2.5 Une *mesure de remédiation* peut être comprise comme une mesure prise pour remédier aux causes sous-jacentes de lacunes ou de carences particulières liées à la sécurité, telles que de la formation. Les mesures de remédiation peuvent consister à restreindre, limiter, suspendre ou révoquer les privilèges d'un titulaire d'autorisation, de certificat ou de licence qui ne continue pas à satisfaire aux qualifications nécessaires pour exercer lesdits privilèges.

7.4.2.6 Bien qu'elles puissent être déclarées comme visant l'un ou l'autre but, de telles mesures peuvent en réalité cibler plusieurs buts. Par exemple, des mesures peuvent être prises par un organisme de réglementation ou par un prestataire de services pour exiger que le titulaire d'une licence ou d'un certificat entreprenne des formations supplémentaires et s'abstienne d'exercer les privilèges de ladite licence ou dudit certificat jusqu'à ce qu'il ait terminé une telle formation avec succès. Des mesures peuvent aussi être prises par un organisme de réglementation pour révoquer, supprimer ou suspendre certains privilèges liés au certificat d'une organisation. De telles mesures relèvent de la remédiation car elles traitent la cause sous-jacente d'un problème de sécurité mais elles peuvent aussi être considérées comme correctrices car elles s'attaquent à une carence particulière. Indépendamment de la caractérisation de la mesure prise, il devrait exister un lien clair et démontrable entre la mesure particulière prise et le maintien ou l'amélioration de la sécurité.

7.4.2.7 Les données de sécurité ou les informations de sécurité pourraient révéler des dangers ou des carences qui nécessiteraient des mesures de remédiation ou de correction aux fins de maintenir la sécurité ou de répertorier des domaines dans lesquels des mesures de prévention amélioreraient la sécurité de l'aviation en traitant des risques potentiels ou émergents. Pour prouver l'existence de la condition ou du danger sous-jacent justifiant la mesure de prévention, de correction ou de remédiation, les États pourraient devoir utiliser les données de sécurité ou les informations de sécurité. Par exemple, des données de sécurité et des informations de sécurité pourraient être requises pour établir la base d'une poursuite administrative concernant une licence ou pour satisfaire à des exigences en matière de charge de la preuve. Des données de sécurité et des informations de sécurité peuvent aussi être nécessaires pour établir le besoin de formation supplémentaire d'un titulaire de licence ou la nécessité de changements dans les systèmes d'un exploitant. Il peut aussi être nécessaire d'utiliser des données de sécurité ou des informations de sécurité pour garantir l'intégrité et le fonctionnement correct du système de compte rendu et du système plus vaste dont il fait partie.

7.4.2.8 En fonction des circonstances, des mesures de prévention, de correction ou de remédiation peuvent être perçues comme punitives par l'individu ou le prestataire de services visé par de telles mesures, alors même que celles-ci n'ont pas vocation à être punitives. En effet, certains peuvent percevoir des mesures relatives à une licence, prises pour pallier des carences de compétences, comme punitives plutôt que comme une mesure nécessaire pour corriger un risque de sécurité ou pour y remédier.

7.4.2.9 Malgré ces perceptions, l'Annexe 19 n'empêche pas les États d'utiliser des données de sécurité et des informations de sécurité à l'appui d'actions requises pour maintenir ou améliorer la sécurité de l'aviation. Lorsque des mesures sont requises pour maintenir ou améliorer le niveau de sécurité de l'aviation ou pour empêcher que le système aéronautique ne se détériore à court terme ou à plus long terme, les États peuvent utiliser des données de sécurité ou des informations de sécurité à l'appui de telles mesures, à condition que ces dernières aient un objectif et un effet démontrables quant à la prévention, la correction ou la remédiation. Dans de tels cas, les États devraient envisager de prendre les mesures nécessaires pour communiquer clairement le raisonnement sous-tendant la mesure prise, afin de prouver le but de sécurité et de réduire au minimum l'incidence négative sur les comptes rendus futurs. Par contre, il devrait être interdit, sauf si un des principes régissant les dérogations s'applique, d'utiliser des données de sécurité et des informations de sécurité pour prendre des mesures dont on ne peut prouver qu'elles visent un ou plusieurs de ces buts et dont on peut démontrer qu'elles ont plutôt un objectif et un effet purement punitifs ou disciplinaires.

7.4.3 Protection des systèmes de compte rendu obligatoire

7.4.3.1 L'Annexe 19 énonce différentes exigences pour la protection des données de sécurité, des informations de sécurité et des sources connexes saisies dans des systèmes de compte rendu volontaire et obligatoire en matière de sécurité. La protection des données de sécurité et des informations de sécurité saisies dans des systèmes de compte rendu volontaire en matière de sécurité est une norme, qui vise à garantir la disponibilité en continu et une plus grande uniformité entre les États, tandis que pour les systèmes de compte rendu obligatoire en matière de sécurité, la disposition prévoyant une telle protection est une pratique recommandée.

7.4.3.2 Dans certaines juridictions, les données de sécurité et les informations de sécurité saisies dans des systèmes de compte rendu obligatoire et volontaire en matière de sécurité font l'objet de différents niveaux de protection, offrant une plus grande protection aux données de sécurité et aux informations de sécurité provenant de systèmes volontaires qu'aux données de sécurité et informations de sécurité provenant de systèmes obligatoires. Cette distinction peut être justifiée par la nécessité d'encourager la fourniture volontaire de données de sécurité ou d'informations de sécurité de manières non perçues comme nécessaires dans le cas d'un système de compte rendu obligatoire.

7.4.3.3 D'autres États offrent le même niveau élevé de protection aux données de sécurité et aux informations de sécurité qu'elles aient été saisies dans des systèmes de compte rendu obligatoire ou volontaire. Cela peut se justifier par la reconnaissance qu'une obligation légale de compte rendu peut ne pas être en elle-même suffisante pour garantir la communication de données de sécurité et d'informations de sécurité pertinentes et qu'un environnement de confiance est une valeur fondamentale de tout type de compte rendu. Étendre les protections aux systèmes de compte rendu obligatoire peut aussi encourager des déclarants à fournir des détails supplémentaires qu'ils ne mentionneraient peut être pas si ces protections n'étaient pas disponibles.

7.4.3.4 Si un État étend la protection accordée aux données de sécurité et aux informations de sécurité saisies dans des systèmes de compte rendu volontaire en matière de sécurité aux systèmes de compte rendu obligatoire en matière de sécurité, les principes régissant la protection et les dérogations contenus dans l'Annexe 19 devraient s'appliquer aux données de sécurité et aux informations de sécurité saisies dans ces deux systèmes ainsi qu'à leurs sources respectives.

7.4.4 Protection des données et des informations dans le domaine public

7.4.4.1 Il se peut que des données de sécurité ou des informations de sécurité soient disponibles dans le domaine public. Dans certains cas, il se peut que de telles données de sécurité ou informations de sécurité ne soient pas sensibles et que leur divulgation ne nuise en rien à la disponibilité en continu de données de sécurité ou d'informations de sécurité. Les données de sécurité et informations de sécurité relatives à la météorologie peuvent être un exemple de telles données et informations non sensibles.

7.4.4.2 Dans d'autres cas, des données de sécurité et informations de sécurité normalement soumises aux principes de protection peuvent tomber dans le domaine public, par exemple, à cause d'une fuite dans les médias. Dans de tels cas, les États devraient s'abstenir de divulguer davantage les données et informations ayant fait l'objet de fuites car les principes de protection ne seront pas automatiquement abandonnés.

7.5 PRINCIPES RÉGISSANT LA PROTECTION

7.5.1 Application des principes régissant la protection

7.5.1.1 La protection des données de sécurité, des informations de sécurité et des sources connexes devrait être la position par défaut de tout État. Les États peuvent prévoir une protection effective au moyen de lois, soutenues par des procédures claires et exhaustives.

7.5.1.2 Le but fondamental d'une protection est de garantir la disponibilité en continu de données de sécurité et d'informations de sécurité en encourageant les individus et les organisations à reconnaître, signaler, analyser et corriger les carences. Pour y parvenir, il faut que toutes les personnes concernées connaissent à l'avance les règles et processus régissant la protection. Ces règles et processus devraient être formalisés et ne devraient pas être susceptibles d'application arbitraire si l'on veut qu'ils servent de base à un système fondé sur la confiance.

7.5.1.3 Lorsque l'on instaure une protection des données de sécurité ou des informations de sécurité, il convient de tenir compte de l'objectif qu'une telle protection doit permettre d'atteindre. Cet objectif peut être évident à la lumière du type de données et d'informations à protéger. Dans de nombreux cas, la protection vise à empêcher que des données de sécurité et des informations de sécurité soient utilisées contre l'individu ou l'organisation qui a signalé ces données ou informations spécifiques. Dans d'autres cas, il peut être important de protéger les données de sécurité ou les informations de sécurité de toute publication ou utilisation générale dans des contextes non liés à la sécurité, tels que des litiges urbanistiques locaux concernant des opérations aéroportuaires et des questions de réduction du bruit.

7.5.1.4 L'action des États est fondamentale pour créer des dispositions de protection. Dans des procédures judiciaires formelles où des règles régissent les preuves qu'il est permis de présenter, seule l'action de l'État peut offrir la protection nécessaire par l'adoption de législations ou de réglementations appropriées qui interdisent ou limitent strictement l'admissibilité des informations protégées. Par exemple, dans des procès au pénal contre un individu, l'utilisation d'un compte rendu volontaire déposé par l'accusé devrait être interdite si elle n'est pas directement liée à l'acte délictueux présumé.

7.5.1.5 Dans des procès au civil contre un prestataire de services, une règle devrait, au minimum, exiger une présomption réfutable[4] que les informations protégées ne peuvent être utilisées. Dans un procès contre une compagnie aérienne pour des dommages encourus à la suite d'un événement, le plaignant peut demander un accès général aux fichiers du SGS de l'exploitant pour tenter de découvrir des informations générales qui pourraient ne pas être directement liées à l'incident mais qui pourraient tendre à présenter l'exploitant sous un jour défavorable. La procédure établie pour trancher de telles questions devrait amener l'autorité compétente (dans ce cas, très probablement un tribunal) chargée d'appliquer les principes régissant les dérogations (exposés plus en détail au § 7.6) à exiger que le plaignant montre précisément quelles informations il entend découvrir et démontre la pertinence de ces informations pour le procès, ainsi que l'absence d'autres sources où obtenir des informations identiques ou similaires. L'autorité compétente pourrait aussi demander au plaignant de montrer en quoi son absence d'accès à ces informations lui porte préjudice. Si la décision est d'accorder un tel accès, des mesures de sauvegarde devraient être imposées par l'autorité compétente conformément aux exigences de procédure applicables, telles que des mesures conservatoires pour empêcher toute publication et pour restreindre l'accès aux parties pertinentes des actes de procédure.

4. Une présomption réfutable est une supposition qui est tenue pour vraie jusqu'à preuve du contraire.

7.5.1.6 Dans des procédures administratives où les qualifications, compétences et capacités techniques ou opérationnelles particulières d'un individu ou d'une organisation sont en question, la sécurité sera presque invariablement au cœur des débats. L'utilisation de données de sécurité ou d'informations de sécurité peut être requise dans de tels cas mais les exigences exécutoires devraient prévoir l'utilisation contrôlée et limitée de telles données et informations. Lorsque les données de sécurité ou les informations de sécurité constituent la base d'une décision dans de tels cas liés à la sécurité, il faudrait tout mettre en œuvre pour veiller à empêcher que l'utilisation desdites données et informations n'induise des conséquences négatives ou préjudiciables pour la source des informations. En général, les individus et organisations qui sont encouragés à rendre compte dans le cadre d'un système de compte rendu protégé reconnaîtront qu'il existe des circonstances dans lesquelles il faut agir dans l'intérêt de la sécurité et que l'action menée doit reposer, en tout ou en partie, sur un compte rendu protégé. Les exigences exécutoires devraient garantir qu'une telle action est conforme au principe fondamental d'équité dans la volonté d'atteindre l'objectif de maintenir ou d'améliorer la sécurité.

7.5.1.7 Un exemple d'une telle situation pourrait être un compte rendu d'un contrôleur de la circulation aérienne qui a perdu connaissance pendant une brève période alors qu'il était à son poste. Il n'y a eu aucune perte de séparation et le compte rendu établi par le contrôleur lui-même est la seule preuve que cet événement s'est produit. À des fins de sécurité, l'analyse de ce compte rendu exige une enquête plus approfondie et, donc, il faut un processus pour rendre l'auteur du compte rendu identifiable. Une mesure de correction immédiate pourrait entraîner le retrait de ce contrôleur du service actif (sans perte financière ni atteinte à la réputation), pendant qu'un examen médical complet et une évaluation médicale sont effectués. Le bilan médical peut se clôturer sur une autorisation médicale, une mise sous traitement médical ou une mise à la retraite pour raison de santé (sans perte financière ni atteinte à la réputation). Si le contrôleur est simplement relevé de ses fonctions, il est hautement improbable que l'on obtienne des comptes rendus similaires d'autres contrôleurs.

7.5.1.8 À ce stade, l'accent a été mis sur les actions directes des États pour assurer la protection nécessaire et appropriée. Dans la pratique, une grande partie des données de sécurité et des informations de sécurité pour lesquelles une protection est requise se trouvent dans l'environnement opérationnel des prestataires de services et font intervenir des relations entre employeurs et employés. Dans ces situations, la protection ne sera pas toujours prévue dans la législation ou dans d'autres formes d'exigences exécutoires de l'État. Toutefois, même dans de tels cas, les États peuvent être en mesure d'exiger une protection effective au moyen de leurs processus de certification, d'approbation et de surveillance continue. L'Annexe 19 exige que des prestataires de services spécifiés mettent en œuvre un SGS efficace. Une gestion efficace de la sécurité repose sur la collecte, l'analyse et la protection des données. Sans données, le système perdrait son efficacité. Le PNS devrait permettre aux États d'ordonner aux organisations de mettre en œuvre des politiques qui assurent une protection à leurs employés dans le cadre de leurs SGS.

7.5.1.9 Une manière de donner une telle protection pourrait être l'anonymisation de l'auteur du compte rendu. Si la confidentialité des comptes rendus est une stratégie utile, une anonymisation complète, lorsqu'elle est possible, élimine la possibilité de réaliser un suivi pendant la phase d'analyse. Les politiques devraient se concentrer sur l'usage que l'autorité compétente pourrait faire ou permettre de faire des données de sécurité et des informations de sécurité en question. L'analyse ci-dessus (voir § 7.5.1.6) relative aux procédures administratives est également applicable au contexte employeur/employé. Ici aussi, les personnes dont il est nécessaire de recevoir des comptes rendus seront peu disposées à fournir de tels comptes rendus si ces comptes rendus, ou d'autres données ou saisies de données, sont utilisés pour étayer une suspension ou un licenciement punitif ou disciplinaire.

7.5.1.10 La saisie de données de sécurité et d'informations de sécurité par des moyens automatiques, tels que les FDR, les enregistreurs de conversations de poste de pilotage ou les enregistreurs vidéo, ou les enregistreurs de données relatives à la gestion du trafic aérien, devrait être couverte par toute politique ou réglementation de protection. L'utilisation de ces dispositifs dans le cadre de la saisie de données des SGS, telle qu'autorisée par la réglementation ou les politiques, doit pleinement respecter les principes de protection, comme c'est le cas pour les comptes rendus volontaires. La confiance de ceux qui rendent compte est indispensable pour assurer une gestion efficace de la sécurité.

7.5.2 Procédures

7.5.2.1 L'Annexe 19 exige que les États veillent à ce que les données de sécurité et les informations de sécurité ne soient pas utilisées dans des procédures disciplinaires, civiles, administratives ou pénales contre des employés, du personnel d'exploitation ou des organisations, sauf si un des principes régissant les dérogations s'applique.

7.5.2.2 Le terme « procédures » peut avoir une portée plus complète et plus large que le terme « action ». Il peut aussi désigner de façon plus étroite les procédures appliquées par un organisme particulier pour revoir ou exécuter des « actions » qui ont été prises par d'autres autorités (ou agences au sein de la même autorité). Au sens général, les termes « procédure » et « action » peuvent être compris comme englobant toutes les démarches entreprises ou toutes les mesures adoptées pour initier, appliquer ou réexaminer une décision d'une autorité qui affecte les droits, privilèges, intérêts légitimes ou attentes raisonnables (tels qu'éventuellement identifiés dans les lois applicables) d'un individu. Vu l'existence de différents systèmes juridiques, la nature et la portée d'actions ou de procédures particulières peuvent varier. Par exemple, dans certains États :

a) Les autorités judiciaires sont généralement associées aux *actions ou procédures au pénal et au civil*. Ces procédures peuvent inclure l'introduction de l'action, la comparution du défendeur, toutes les démarches auxiliaires ou provisoires, les plaidoiries, les enquêtes préalables au procès et d'autres enquêtes formelles. À la suite de telles actions ou procédures, une personne peut être condamnée au paiement de dommages-intérêts, d'une amende ou, dans certains cas, à une peine de prison.

b) Des *actions ou procédures administratives* peuvent amener une enquête, des investigations ou une audience devant une autorité de réglementation ou un tribunal à modifier, suspendre, révoquer ou annuler une autorisation (dans certains cas, à des fins manifestement liées à la sécurité, dans d'autres, à des fins punitives).

c) Des *actions ou procédures disciplinaires* peuvent désigner le processus par lequel un employeur réagit à des violations ou transgressions, réelles ou manifestes, des règles et procédures, par un employé. De telles actions ou procédures peuvent aboutir à l'exonération de l'employé supposé avoir commis une faute ou à la prise de mesures disciplinaires ou au congédiement de ce dernier si les allégations s'avèrent fondées.

7.5.2.3 D'autres autorités peuvent être associées aux actions et procédures susmentionnées, notamment des tribunaux administratifs, des organismes professionnels ou éthiques ou d'autres organes de contrôle au sein d'une organisation.

7.5.2.4 Il importe de se rappeler que les principes de protection ne s'appliquent pas lorsque des États entreprennent une action de prévention, de correction ou de remédiation qui est nécessaire au maintien ou à l'amélioration de la sécurité de l'aviation (voir § 7.4.2 ci-dessus). Cette remarque vaut aussi pour toute procédure, action ou mesure liée à une action de prévention, de correction ou de remédiation entreprise aux fins de maintenir ou d'améliorer la sécurité. Par exemple, l'utilisation de données de sécurité ou d'informations de sécurité pour justifier l'adoption d'une action de prévention, de correction ou de remédiation est autorisée dans des procédures entamées à l'initiative d'un individu ou d'une organisation qui tente de contester ladite action.

7.5.2.5 Alors qu'il peut exister des cas dans lesquels des données de sécurité ou des informations de sécurité sont utilisées dans des actions en justice entamées par un tiers contre la source du compte rendu, les États sont encouragés à prendre toutes les mesures nécessaires pour veiller à ce que lesdites données de sécurité et informations de sécurité ne soient pas utilisées à d'autres fins que le maintien ou l'amélioration de la sécurité de l'aviation (à moins qu'un des principes régissant les dérogations ne s'applique).

7.5.3 Mesures de protection qui font autorité

7.5.3.1 Certains facteurs peuvent atténuer les conséquences négatives associées à la divulgation ou à l'utilisation de données de sécurité ou d'informations de sécurité à d'autres fins que le maintien ou l'amélioration de la sécurité de l'aviation. Il pourrait être possible de limiter tout préjudice potentiel découlant de la divulgation ou de l'utilisation proposée en mettant en place des mesures de protection qui limitent encore la divulgation ou l'utilisation de données de sécurité et d'informations de sécurité. Dans leurs législations ou réglementations en vertu desquelles l'application des principes régissant les dérogations est envisagée, les États peuvent prévoir que l'autorité compétente est habilitée à imposer des exigences pour préserver la confidentialité des données de sécurité ou des informations de sécurité après une décision d'autoriser l'accès.

7.5.3.2 L'anonymisation de la source des données de sécurité et des informations de sécurité est une autre mesure de protection qui peut être utilisée avant qu'une autorité compétente n'accorde l'autorisation de divulguer ces données et informations à d'autres fins que le maintien ou l'amélioration de la sécurité de l'aviation. L'anonymisation peut toutefois être difficile lorsque les sources fournissant les données de sécurité ou les informations de sécurité sont déjà identifiables à partir du contenu des données ou informations communiquées. Par exemple, le compte rendu d'un événement concernant un type d'aéronef utilisé par un seul exploitant dans une juridiction spécifique peut immédiatement révéler cet exploitant (voire un employé particulier) simplement par l'identification du type d'aéronef concerné. Dans de tels cas, la façon et le lieu où l'on propose de divulguer ou utiliser lesdites données de sécurité ou informations de sécurité, et la nature des informations concernées, revêtiraient une importance particulière.

7.5.3.3 S'il est proposé d'utiliser les données de sécurité ou les informations de sécurité dans un forum où la connaissance des personnes ou organisations liées auxdites données ou informations est limitée, l'autorité compétente pourrait avoir l'assurance que l'anonymisation fournirait une mesure de protection suffisante pour les sources. De même, si la nature des informations est essentiellement technique, les données et informations de sécurité ne contiendront peut-être pas beaucoup d'informations d'identification à supprimer ou à modifier, ce qui rend la tâche de protection plus facile à exécuter. L'autorité compétente devrait aussi se demander si le forum où il est proposé de divulguer les données ou informations ou si l'utilisation desdites données et informations et la nature de ces informations affecteront la mesure dans laquelle les sources peuvent être identifiées, et si la suppression des informations d'identification serait une mesure suffisante. Si la divulgation ou l'utilisation proposée est susceptible d'avoir une incidence négative sur une organisation ou une entreprise, telle qu'un exploitant aérien, l'autorité compétente devrait décider si l'anonymisation des données ou informations fournirait une protection raisonnable, similaire à celle qu'aurait obtenue la société ou l'exploitant si la divulgation ou l'utilisation n'avait pas été autorisée.

7.5.3.4 Si l'autorité compétente estime que l'anonymisation des données de sécurité et des informations de sécurité peut prévenir l'utilisation volontaire ou permissible de données de sécurité ou d'informations de sécurité, l'anonymisation ne sera pas appropriée. C'est pourquoi les États peuvent choisir de mettre en œuvre différents types de mesures de protection (ou des combinaisons de mesures de protection), afin de permettre une divulgation limitée dans un but spécifique, tout en empêchant une utilisation plus large des données de sécurité ou des informations de sécurité ou leur divulgation au public. Des mesures conservatoires, des procédures à huis clos, des examens et résumés en chambre sont autant d'exemples de telles mesures de protection.

7.5.3.5 Les États et organisations peuvent aussi adopter des bonnes pratiques, notamment veiller à ce que l'environnement dans lequel les informations sont collectées, stockées, traitées et transmises soit suffisamment sûr, et à ce que les contrôles portant sur l'accès et sur les autorisations soient suffisants pour protéger les données de sécurité et les informations de sécurité.

7.6 PRINCIPES RÉGISSANT LES DÉROGATIONS

7.6.1 Les principes régissant la protection s'appliquent aux données de sécurité, aux informations de sécurité et aux sources connexes, à moins qu'une autorité compétente ne stipule qu'un des trois principes régissant les

dérogations s'applique. Le gardien du SDCPS devrait connaître les protections appliquées aux données de sécurité, aux informations de sécurité et à leurs sources connexes et devrait veiller à ce que leur divulgation et leur utilisation se fassent conformément aux dispositions de l'Annexe 19.

7.6.2 Désignation d'une autorité compétente

7.6.2.1 Étant donné que les principes régissant les dérogations seront administrés pour un éventail de buts différents, l'autorité compétente variera selon la nature des données ou des informations concernées et selon le type d'usage recherché. Dans chaque cas particulier, la tâche de l'autorité compétente sera de décider si un principe particulier régissant les dérogations s'applique. L'autorité compétente devra être en mesure de trouver un juste équilibre entre des intérêts divergents, tels que les lois relatives au droit à l'information, les réglementations non liées à la sécurité de l'aviation, les règles de divulgation en cas d'actions en justice, et d'autres règles, afin que le public ait confiance dans ses capacités décisionnelles. Les autorités compétentes pourraient comprendre les autorités judiciaires, les autorités de réglementation ou d'autres autorités chargées de responsabilités aéronautiques, désignées en application des lois nationales et autres exigences exécutoires.

7.6.2.2 Les États et les organisations devront identifier des autorités compétentes appropriées pour appliquer les principes régissant les dérogations à différents buts. Le Tableau 9 ci-dessous cite des exemples d'autorités compétentes possibles et des exemples de situations.

Tableau 9. Exemples de situations et d'autorités compétentes possibles

Exemple de situation	*Autorité compétente possible*
La divulgation ou l'utilisation de données de sécurité ou d'informations de sécurité est demandée par un membre du public en application des lois régissant le droit à l'information[5].	Département ministériel ou instance administrative
Si la question de la divulgation ou de l'utilisation des données ou des informations devient en elle-même l'objet d'une action en justice entamée en application des mêmes lois sur le droit à l'information, ou si les données de sécurité ou les informations de sécurité sont demandées pour utilisation dans le cadre de procédures judiciaires.	Tribunal ou tribunal administratif
Si l'action doit être entreprise par une autorité de réglementation pour maintenir ou améliorer la sécurité.	AAC
Dans le cas d'une divulgation ou d'une utilisation de données de sécurité ou d'informations de sécurité dont une organisation est dépositaire.	Le responsable de l'organisation qui est chargé de la sécurité de l'aviation, tel qu'un cadre dirigeant ou un groupe d'experts constitué de membres de la direction, d'un représentant des employés et, dans certains États, d'un représentant de l'autorité de réglementation

5. Pour plus d'informations concernant les lois régissant le droit à l'information, voir le § 7.7 du présent chapitre.

7.6.2.3 Lorsqu'une organisation identifie son autorité compétente, l'exercice responsable du pouvoir discrétionnaire de l'autorité compétente concernant l'application des principes régissant les dérogations et des principes régissant la protection pourrait assurer une autodiscipline suffisante au sein de l'organisation. La détermination finale de l'autorité compétente pour chaque but spécifique reste un privilège de chaque État et organisation, en fonction des lois et politiques applicables.

7.6.2.4 Une désignation permanente du bureau et de la juridiction de l'autorité compétente (p. ex. autorités judiciaires pour des questions faisant l'objet d'actions en justice, l'AAC pour des questions visées par des mesures réglementaires) peut être envisagée pour permettre un processus décisionnel plus rapide. Une désignation permanente offrira en outre une certitude quant au droit d'agir et à l'expérience de l'autorité compétente pour décider de ces questions. Par ailleurs, il est crucial que l'autorité compétente ait mis en place des règles et procédures régissant le processus décisionnel. Ces règles et procédures devraient découler des lois nationales applicables. La mise en place de telles règles et procédures n'est réalisable que si la désignation de l'autorité compétente dans un domaine particulier reste constante.

7.6.3 Application des principes régissant les dérogations

7.6.3.1 Le premier cas dans lequel une autorité compétente peut estimer qu'une dérogation à la règle de protection s'applique est celui où il existe « des faits et circonstances qui laissent raisonnablement présumer que l'événement pourrait avoir été causé par un acte ou une omission considérés, d'après les lois nationales, comme un cas de négligence grave, une faute intentionnelle, ou un acte criminel ». L'autorité compétente appropriée pour déterminer cela sera, le plus souvent, une instance judiciaire, administrative ou une instance chargée des poursuites.

7.6.3.2 Étant donné qu'une évaluation quant au fond des données de sécurité ou des informations de sécurité en question déterminera souvent si la conduite concernée satisfait à l'une ou l'autre des conditions d'usage exceptionnel, il n'est pas nécessaire que les faits et circonstances du cas démontrent sans équivoque qu'une telle conduite exceptionnelle s'est produite. En fait, il est seulement nécessaire que ces faits et circonstances fournissent une base raisonnable permettant d'estimer que l'événement pourrait avoir été causé par une telle conduite. Si l'autorité compétente détermine que, sur la base des faits et circonstances d'un cas, un événement peut avoir été le résultat soit d'une négligence grave, d'une faute intentionnelle ou d'un acte criminel — dans l'acception donnée à ces termes dans le droit national — un des principes régissant les dérogations s'applique et les données de sécurité, informations de sécurité ou sources connexes peuvent être mises à disposition.

7.6.3.3 Des systèmes juridiques différents peuvent, en vertu du droit national, donner des acceptions différentes à ces termes. En général, on entend par négligence grave un acte ou une omission commis avec un mépris ou une indifférence grave pour un risque manifeste, que ce risque ait été totalement évalué par l'auteur ou non. De tels actes ou omissions sont parfois qualifiés de conduite imprudente. Une faute intentionnelle est un acte ou une omission illicite dont l'auteur connaît le caractère illicite ou est sciemment indifférent à la question de savoir si l'acte ou l'omission est oui ou non licite. Dans ces cas, la connaissance et l'intention peuvent aussi parfois concerner les conséquences d'une telle conduite, par opposition à sa description formelle comme illicite. Quoi qu'il en soit, les vérifications des éléments de preuve et les mesures applicables pour déterminer la nature de la conduite concernée devraient être cohérentes avec les lois de la juridiction pertinente. En outre, comme les principes régissant les dérogations établissent une distinction entre les conduites qui constituent une « négligence grave » ou une « faute intentionnelle », d'une part, et un « acte criminel », d'autre part, il est clair qu'une conduite qui pourrait constituer soit une « négligence grave » ou « une faute intentionnelle » (quelle que soit la description de cette conduite donnée dans le droit national applicable) doit être évaluée sur la base d'une norme civile et non pénale.

7.6.3.4 Le deuxième cas dans lequel une autorité compétente peut déterminer qu'une dérogation à la règle de protection s'applique est celui où, après examen des données de sécurité ou des informations de sécurité en question, l'autorité compétente estime que la mise à disposition de ces données ou informations est « nécessaire à l'administration appropriée de la justice » et « que les avantages de cette mise à disposition l'emportent sur les incidences défavorables qu'elle pourrait avoir, aux niveaux national et international, sur la collecte et la disponibilité futures des données de sécurité et des informations de sécurité ».

7.6.3.5 La décision est prise au terme d'un processus d'évaluation en deux étapes, dans lequel l'autorité compétente doit examiner d'abord si les données ou les informations sont « nécessaires à l'administration appropriée de la justice », ce qui ne sera peut-être pas le cas si les mêmes informations sont disponibles auprès d'autres sources ; ensuite, si elle estime que la mise à disposition est nécessaire à l'administration appropriée de la justice, elle doit examiner, après avoir pesé le pour et le contre, si la valeur de ces données ou informations l'emporte sur le préjudice que leur mise à disposition portera probablement à la collecte et à la disponibilité futures de données de sécurité et d'informations de sécurité aux fins du maintien ou de l'amélioration de la sécurité.

7.6.3.6 Si les données de sécurité ou les informations de sécurité sont proposées pour mise à disposition dans une action ou une procédure en justice (de nature civile, administrative, pénale ou disciplinaire), l'incidence négative potentielle d'une telle mise à disposition peut concerner la source desdites données ou informations. Même si des mesures de protection peuvent être mises en place pour empêcher que les données de sécurité ou les informations de sécurité soient divulguées en dehors des limites de l'action ou de la procédure en justice, toute incidence négative de la mise à disposition desdites données ou informations pendant une procédure pourrait malgré tout décourager de futurs comptes rendus ou divulgations de données de sécurité et d'informations de sécurité aux fins du maintien ou de l'amélioration de la sécurité. Si la mise à disposition proposée des données de sécurité ou des informations de sécurité implique la diffusion ou la publication desdites données ou informations au-delà des limites de la procédure, l'autorité compétente devrait aussi envisager l'effet préjudiciable potentiel sur l'ensemble de la communauté (nationale et internationale).

7.6.3.7 Au niveau individuel, le fait de rendre ces informations publiques peut porter préjudice à la personne concernée, en provoquant embarras et/ou perte potentielle de moyens de subsistance. À un niveau plus large, la publication ou la diffusion de données de sécurité ou d'informations de sécurité dans une affaire particulière peut avoir un effet dissuasif général sur des personnes dans des situations similaires mais non concernées par l'action ou la procédure en question, personnes qui seront dès lors peu enclines à communiquer de telles données ou informations ou à contribuer à leur collecte.

7.6.3.8 Lorsqu'elle prend une décision concernant les deux premiers principes régissant les dérogations, l'autorité compétente doit avoir la certitude que :

a) dans le premier cas, le contenu des données de sécurité ou des informations de sécurité que l'on cherche à divulguer ou à utiliser est nécessaire pour décider si un acte ou une omission constitue une négligence grave, une faute intentionnelle ou un acte criminel ;

b) dans le deuxième cas, de telles données, informations ou leurs sources connexes sont nécessaires à l'administration appropriée de la justice.

7.6.3.9 L'autorité compétente déterminera si les données de sécurité, les informations de sécurité ou l'identité de la source desdites données ou informations sont nécessaires pour juger de l'affaire. Si une autorité compétente peut raisonnablement prendre une décision sans faire référence aux données, informations ou sources protégées, il faut alors donner plus de poids à la préservation de la protection desdites données de sécurité, informations de sécurité et sources connexes. Il n'est pas nécessaire de nuire à la collecte et à la disponibilité de données de sécurité, d'informations de sécurité et aux sources connexes lorsqu'une décision peut être prise par l'autorité compétente sans demander la divulgation (ou l'utilisation) de telles données et informations. Cela contribuera à garantir la disponibilité en continu de données de sécurité et d'informations de sécurité aux fins du maintien ou de l'amélioration de la sécurité de l'aviation.

7.6.3.10 Des conséquences néfastes pourraient découler de la divulgation ou de l'utilisation de données de sécurité, d'informations de sécurité et de leurs sources connexes, notamment la réticence du personnel d'exploitation de l'aviation à coopérer volontairement avec les inspecteurs. Si de tels données, informations ou détails sur leurs sources ne sont pas nécessaires pour prouver un fait essentiel dans une procédure en justice, il ne faut donc pas compromettre la collecte et la disponibilité futures de données de sécurité, d'informations de sécurité et de leurs sources connexes par une mise à disposition inutile au titre de l'un ou l'autre de ces principes régissant les dérogations. De plus, si les

informations requises peuvent être aisément obtenues d'autres sources, l'autorité compétente pourrait décider de ne pas autoriser l'accès aux données de sécurité ou aux informations de sécurité tant que tous les autres moyens raisonnables d'obtenir ces informations n'ont pas été épuisés.

7.6.3.11 De même, si, dans un État qui n'a pas de loi sur le droit à l'information, il est demandé à une autorité compétente de décider si les données de sécurité ou les informations de sécurité devraient être divulguées au grand public (p. ex. en réponse à une demande des médias), l'autorité compétente voudra très probablement savoir dans quelle mesure il est important que le grand public connaisse le contenu desdites données ou informations. Dans une telle situation, l'autorité compétente pourrait poser une question telle que : « Sans connaître le contenu de ces données ou informations, le public aurait-il une compréhension correcte de l'événement ou cet événement aurait-il des conséquences pour la sécurité des voyageurs ? » Pouvoir prouver que, sans accès à ces données de sécurité ou ces informations de sécurité, la compréhension du grand public serait compromise peut donner plus de poids à une argumentation en faveur de leur divulgation. Toutefois, ces données ou informations ne devraient pas être divulguées uniquement parce que ces motifs sont établis. Si la divulgation risquait de compromettre gravement la disponibilité en continu de données de sécurité et d'informations de sécurité en décourageant de futurs comptes rendus en matière de sécurité, la balance ne pencherait pas nécessairement en faveur d'une divulgation.

7.6.3.12 Le troisième type de dérogation concerne les cas dans lesquels « après examen des données de sécurité ou des informations de sécurité », l'autorité compétente « établit que leur mise à disposition est nécessaire pour maintenir ou améliorer la sécurité et que les avantages de cette mise à disposition l'emportent sur les incidences défavorables qu'elle pourrait avoir, aux niveaux national et international, sur la collecte et la disponibilité futures des données de sécurité et des informations de sécurité ». Cette dérogation s'applique à la mise à disposition des données de sécurité ou des informations de sécurité nécessaires au maintien ou à l'amélioration de la sécurité. Elle ne s'applique pas à l'utilisation de données de sécurité ou d'informations de sécurité en lien avec des mesures de prévention, de correction ou de remédiation prises par une autorité de réglementation et qui sont nécessaires au maintien ou à l'amélioration de la sécurité de l'aviation.

7.6.3.13 Les circonstances envisagées par l'Annexe 19 couvrent la prise en considération, par une autorité compétente, des avantages d'une mise à disposition de données de sécurité ou d'informations de sécurité pour des buts plus généraux liés au maintien ou à l'amélioration de la sécurité, notamment à des fins de formation et d'enseignement ou pour une publication d'informations de sécurité et de conseils au bénéfice de l'ensemble de la communauté. L'analyse de ces situations se fait selon le type de processus en deux étapes décrit au § 7.6.3.5 ci-dessus : tout d'abord, il faut que l'autorité compétente décide que « la mise à disposition est nécessaire pour maintenir ou améliorer la sécurité » et, ensuite, il faut que l'autorité compétente établisse que les avantages de la mise à disposition des données de sécurité ou des informations de sécurité l'emportent sur les incidences défavorables qu'une telle mise à disposition pourrait avoir sur la collecte et la disponibilité futures de telles données et informations.

7.6.3.14 Dans l'examen de la deuxième étape de cette analyse, l'Annexe 19 encourage les autorités compétentes à tenir compte du « consentement de la source des données de sécurité et des informations de sécurité ». L'importance de cette reconnaissance souligne la distinction cruciale évoquée au § 7.4.2 ci-dessus, entre la mise à disposition de données de sécurité et d'informations de sécurité à des fins généralement liées au maintien ou à l'amélioration de la sécurité (auquel cas ce principe régissant les dérogations sera d'application), et l'utilisation des données de sécurité et des informations de sécurité à des fins de prévention, de correction et de remédiation particulières, à l'appui du maintien ou de l'amélioration de la sécurité (auquel cas il ne sera pas nécessaire de satisfaire aux exigences de l'un quelconque des principes régissant les dérogations car cet usage est déjà autorisé dans le cadre des principes régissant la protection).

7.6.3.15 Conformément à l'esprit des principes régissant la protection, lorsqu'elle envisage l'utilisation de données de sécurité ou d'informations de sécurité à l'appui de mesures de prévention, de correction ou de remédiation prises pour maintenir ou améliorer la sécurité, l'autorité compétente a la possibilité de s'assurer de la disponibilité concrète d'une éventuelle autre source appropriée pour ces données ou informations. Si une telle autre source existe, même cette mise à disposition non exceptionnelle de données de sécurité ou d'informations de sécurité protégées peut être évitée.

7.6.3.16 Toutefois, l'examen de cette possibilité n'exige ni n'encourage l'application formelle d'un des principes régissant les dérogations évoqués dans l'Annexe 19. La raison en est qu'un des principes régissant les dérogations s'applique lorsque l'intérêt de maintenir ou d'améliorer la sécurité est mis en balance avec d'autres intérêts publics divergents (p. ex. l'administration appropriée de la justice, l'offre d'un libre accès aux données ou informations, ou la facilitation des processus de formation ou d'enseignement par une autorisation d'inclure des données ou informations protégées). Les mesures de prévention, de correction ou de remédiation prises aux fins de maintenir ou d'améliorer la sécurité relèvent du champ d'application des principes régissant la protection et il n'existe aucun intérêt contraire, non lié à la sécurité, avec lequel une telle utilisation devrait être mise en balance.

7.6.4 Considérations supplémentaires pour l'application d'un des principes régissant les dérogations

7.6.4.1 Pour établir si un des principes régissant les dérogations s'applique dans un cas, l'autorité compétente devrait toujours tenir compte du consentement de la source des données de sécurité ou des informations de sécurité. Si une personne a reçu des assurances quant au respect de la confidentialité des données de sécurité ou des informations de sécurité dont elle est la source, toute utilisation, divulgation ou mise à disposition desdites données ou informations qui serait contraire à ces assurances risque d'avoir une incidence négative sur les données de sécurité et les informations de sécurité qui pourraient être fournies par cette personne à l'avenir. De plus, si les données de sécurité ou les informations de sécurité devaient être mises à disposition ou utilisées malgré les assurances de confidentialité données à la source, cela pourrait aussi avoir une incidence négative sur toute personne susceptible de prendre connaissance de ce fait.

7.6.4.2 Pour éviter la survenance de situations non souhaitables telles que celles mentionnées au § 7.6.4.1, il sera prudent de s'assurer que les individus et les organisations comprennent clairement à l'avance comment, quand, où et dans quels buts les données et informations qu'ils fournissent peuvent être utilisées conformément à l'application des principes régissant les dérogations. Cette compréhension est cruciale pour établir et maintenir un environnement de compte rendu prévisible, basé sur la confiance.

7.6.4.3 La Figure 7-2 illustre des éléments indicatifs généraux conformes aux dispositions de l'Annexe 19, concernant l'application, par l'autorité compétente, des principes régissant les dérogations[6].

7.7 DIVULGATION AU PUBLIC

7.7.1 Les données de sécurité ou informations de sécurité relèvent de l'intérêt général. Ouverture, transparence et obligation de rendre compte sont dans l'intérêt de tous, afin que le public ait une conscience générale de la sécurité du système et puisse recevoir la garantie que tout le nécessaire est fait pour gérer la sécurité. Des individus ou des groupes d'intérêt spécifiques peuvent aussi s'intéresser aux données de sécurité ou aux informations de sécurité pour des motifs autres que ceux qui sont directement liés à la sécurité. La divulgation peut se faire volontairement, à la suite d'une demande d'information adressée au gouvernement, ou dans le cadre des processus d'une action judiciaire. La pertinence de divulguer ou non des données de sécurité ou des informations de sécurité au grand public dépend de la nature de ces données de sécurité et informations de sécurité. Il appartient à l'autorité compétente d'établir cette pertinence, comme indiqué précédemment.

6. Il est important de ne pas oublier que les États ne sont pas empêchés d'*utiliser* des données de sécurité ou des informations de sécurité pour prendre des mesures de prévention, de correction ou de remédiation nécessaires au maintien ou à l'amélioration de la sécurité de l'aviation.

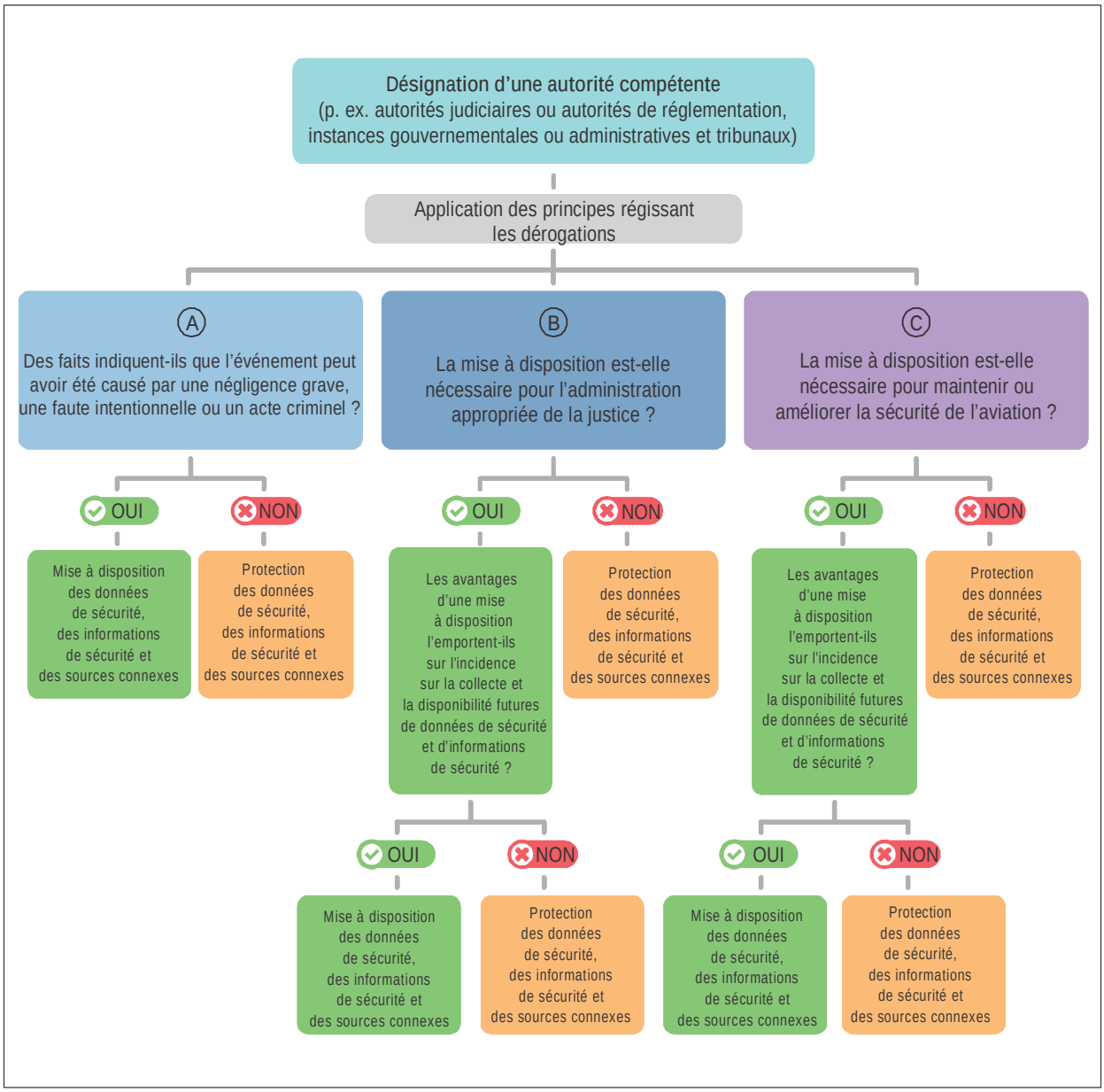

Figure 7-2. Éléments indicatifs pour l'application des principes régissant les dérogations

7.7.2 Si des données de sécurité ou des informations de sécurité sont divulguées au grand public, il n'est généralement pas possible de limiter les modalités d'utilisation de ces informations. Certes l'ouverture et la transparence devraient être encouragées mais, parallèlement, il convient de tenir compte des droits et attentes légitimes de ceux qui ont participé aux comptes rendus et analyses des données de sécurité et informations de sécurité, et de la nécessité de les protéger d'atteintes inappropriées à leurs intérêts ou à leur réputation. Cependant, cette remarque ne s'applique pas toujours aux États ayant des lois sur le droit à l'information.

7.7.3 Nombre d'États ont une législation qui, dans les faits, oblige à divulguer toutes les informations détenues par les institutions de l'État. De telles lois sont parfois appelées lois sur le droit à l'information. En vertu de ces lois, hormis en cas de dérogation pour un type particulier d'informations, les informations doivent être divulguées par

le gouvernement, sur demande. Les dérogations peuvent concerner, entre autres, des informations classifiées, des informations sensibles sur le plan commercial ou des informations telles que des dossiers médicaux, qui sont protégés par les lois relatives à la protection de la vie privée. Les données de sécurité ou les informations de sécurité ne font généralement pas l'objet de dérogations. Conformément à l'Annexe 19, les États peuvent choisir de créer des dérogations ou des règles visant à protéger ces données et informations d'une divulgation au public en application de lois sur le droit à l'information ou de tout autre type de loi, y compris la législation aéronautique.

7.7.4 Les lois sur le droit à l'information s'appliquent généralement aux informations détenues par le gouvernement. Étant donné que la plupart des données de sécurité et des informations de sécurité nécessitant une protection contre toute divulgation sont obtenues auprès du personnel d'exploitation ou d'un prestataire de services, une approche pratique serait de permettre que lesdites données et informations restent au sein de l'organisation au lieu d'être déposées auprès d'une autorité gouvernementale. Ainsi, la question de la divulgation au public ne se pose pas, sauf si des actions gouvernementales supplémentaires, telles qu'une procédure administrative, sont entamées. Lorsque la question de la divulgation au public se pose dans une procédure administrative ou judiciaire, l'autorité compétente devrait appliquer les principes de base régissant la protection, évoqués plus haut. Cette approche pourrait ne pas fonctionner si des prestataires de services sont obligés de communiquer des données de sécurité et des informations de sécurité à une autorité gouvernementale, ou si le prestataire de services est une autorité ou une instance gouvernementale ou fait partie d'une telle autorité ou instance.

7.7.5 Une incapacité à évaluer correctement les demandes conflictuelles d'accès aux données de sécurité ou aux informations de sécurité peut influer de deux manières sur les efforts actuels et futurs. La divulgation au public de certaines données ou informations peut être perçue comme une violation de la vie privée d'individus ou des attentes de confidentialité d'organisations associées à ces données de sécurité ou informations de sécurité. L'utilisation de certaines données ou informations dans le cadre d'une argumentation à l'appui de sanctions contre des individus ou des organisations concernés peut être perçue comme une violation des principes d'équité fondamentaux. La disponibilité future de données de sécurité et d'informations de sécurité pourrait en pâtir, vu la propension humaine à ne pas divulguer des informations en cas de crainte que leur divulgation ou un usage compromettant ne génère une menace. Cela peut avoir une incidence négative évidente sur les fonctions de la gestion de la sécurité touchant tant à la collecte qu'à l'analyse des données.

7.7.6 Si une autorité compétente établit que les données de sécurité ou les informations de sécurité peuvent être divulguées au public, l'État doit s'assurer que toute divulgation au public soit faite dans le respect des lois applicables sur la protection de la vie privée ou sous une forme anonymisée, résumée ou agrégée. Le § 7.5.3 fournit de plus amples informations sur les mesures de protection qui font autorité.

7.8 PROTECTION DES DONNÉES ENREGISTRÉES

7.8.1 Protection des enregistrements de l'ambiance sonore sur les lieux de travail

7.8.1.1 Les enregistrements de l'ambiance sonore sur les lieux de travail devraient faire partie de toute politique ou réglementation régissant la protection. L'utilisation de ces enregistrements dans le cadre de la gestion de la sécurité là où la réglementation ou la politique le permet devrait pleinement respecter les principes régissant la protection et les dérogations. La confiance de ceux qui rendent compte est indispensable pour assurer une gestion efficace de la sécurité. Cette confiance ne devrait jamais être mise en péril.

7.8.1.2 Les dispositions contenues dans l'Annexe 19 sont applicables aux fonctions de la gestion de la sécurité relatives à ou à l'appui direct de l'exploitation sûre des aéronefs. Les enregistrements de l'ambiance sonore sur les lieux de travail peuvent être régis par les lois nationales sur la protection de la vie privée qui ne sont pas définies dans l'Annexe 19.

7.8.1.3 Les enregistrements de l'ambiance sonore sur les lieux de travail peuvent inclure les CVR, les AIR, d'autres enregistrements réalisés avec des enregistreurs de bord, ou des enregistrements de communications en arrière-plan et l'environnement sonore aux postes de travail des contrôleurs de la circulation aérienne.

7.9 PARTAGE ET ÉCHANGE DES INFORMATIONS DE SÉCURITÉ

7.9.1 Protection des informations partagées entre États

7.9.1.1 Étant donné qu'un des objectifs principaux du partage et de l'échange des informations de sécurité est de garantir une réaction cohérente, factuelle et transparente à des préoccupations en matière de sécurité au niveau de l'État et au niveau mondial, les États agiront conformément aux principes suivants, dans le processus de partage et d'échange d'informations de sécurité :

a) le respect de la Convention relative à l'aviation civile internationale (Convention de Chicago), de ses Annexes et d'autres obligations multilatérales et bilatérales des États ;

b) le partage et l'échange d'informations de sécurité n'entraînent pas de violation, par les autorités compétentes de l'État, des lois nationales relatives à la protection des informations de sécurité, y compris, mais sans s'y limiter, les lois et réglementations nationales sur le secret d'État, la protection des données à caractère personnel, le secret commercial (industriel), ni de violation des droits des personnes physiques et morales ;

c) les informations de sécurité partagées et échangées par un État ne devraient pas être utilisées d'une manière qui influe négativement sur l'État lui-même, ses compagnies aériennes, ses fonctionnaires et ses citoyens ainsi qu'à d'autres fins inappropriées, notamment pour gagner un avantage économique ;

d) l'unique but de la protection des informations de sécurité contre une utilisation inappropriée est d'assurer la disponibilité en continu de ces informations afin que des mesures de prévention appropriées et opportunes puissent être prises et que la sécurité de l'aviation puisse être renforcée ;

e) le partage et l'échange d'informations de sécurité devraient se faire conformément aux principes régissant la protection, énoncés à l'Annexe 19.

7.9.1.2 Un cadre juridique pour le partage et l'échange d'informations peut reposer sur des accords bilatéraux entre États, insérés, par exemple, dans leurs accords relatifs au transport aérien (aux services aériens). Pour faciliter le partage et l'échange d'informations, les États peuvent aussi convenir que de tels accords bilatéraux sont provisoirement d'application, le cas échéant, dans l'attente de leur ratification et entrée en vigueur.

7.9.1.3 Les États devraient promouvoir et faciliter l'établissement de réseaux pour le partage et l'échange d'informations de sécurité entre les usagers du système aéronautique. Le partage et l'échange d'informations de sécurité sont fondamentaux pour garantir une réaction cohérente, factuelle et transparente à des préoccupations en matière de sécurité au niveau de l'État et au niveau mondial.

Chapitre 8

GESTION DE LA SÉCURITÉ PAR LES ÉTATS

8.1 INTRODUCTION

8.1.1 Le Chapitre 3 de l'Annexe 19 contient des SARP relatives aux responsabilités des États en matière de gestion de la sécurité. Parmi ces responsabilités figurent l'établissement et la tenue à jour d'un programme national de sécurité (PNS) destiné à assurer une gestion intégrée de la sécurité.

8.1.2 La première édition de l'Annexe 19 exigeait des États qu'ils établissent et mettent en œuvre deux ensembles de dispositions, à savoir les huit éléments cruciaux (EC) d'un système national de supervision de la sécurité (SSO) et les quatre composants d'un PNS. Le volet relatif à la supervision de la sécurité reflétait le rôle traditionnel de l'État, qui est de garantir la mise en œuvre efficace des SARP normatives par l'industrie aéronautique, tandis que le PNS représentait l'intégration des principes de gestion de la sécurité. Les détails des huit éléments cruciaux figuraient à l'Appendice 1 de l'Annexe avec le statut de SARP ; les éléments détaillés d'un cadre pour la mise en œuvre et la tenue à jour d'un PNS étaient fournis au Supplément A, à titre d'éléments indicatifs.

8.1.3 Le système de supervision de la sécurité et le PNS étaient étroitement liés en ce qui concerne les objectifs de sécurité que chacun vise à atteindre. Les deux abordent les fonctions et responsabilités de l'État ; le premier, principalement en matière de supervision de la sécurité, l'autre, en matière de gestion de la sécurité et de performance de sécurité. À l'évidence, certains aspects de la gestion de la sécurité dans les huit EC reflètent la transition vers une approche proactive de la gestion de la sécurité. Par exemple, les obligations de surveillance (EC-7) peuvent être considérées comme un élément de l'assurance de la sécurité, et la législation aéronautique de base (EC-1) et les règlements d'exploitation spécifiques (EC-2) étaient aussi reflétés dans le cadre original des PNS en tant qu'importants mécanismes de maîtrise des risques de sécurité.

8.1.4 Ces responsabilités ont été intégrées dans la deuxième édition de l'Annexe 19 et sont collectivement appelées les responsabilités de l'État en matière de gestion de la sécurité. Les SARP relatives aux responsabilités de l'État en matière de gestion de la sécurité, qui couvrent à la fois la supervision de la sécurité et la gestion de la sécurité, sont interdépendantes et constituent une approche intégrée visant une gestion efficace de la sécurité. Bien que l'abréviation PNS soit encore utilisée dans la deuxième édition de l'Annexe 19, son sens a changé pour englober l'ensemble intégré des SARP figurant au Chapitre 3. En tant que tel, le PNS n'est plus décrit comme un cadre mais plutôt comme un programme visant à permettre aux États d'assumer leurs responsabilités en matière de gestion de la sécurité, programme qui inclut aussi la supervision de la sécurité. Ainsi, le PNS fait partie du concept large de gestion de la sécurité par les États. Cette évolution est illustrée à la Figure 8-1.

8.2 PROGRAMME NATIONAL DE SÉCURITÉ (PNS)

8.2.1 Éléments cruciaux d'un système national de supervision de la sécurité

Les EC d'un système national de supervision de la sécurité (SSO) constituent la base du PNS. La deuxième édition de l'Annexe 19 souligne l'importance d'un système de supervision de la sécurité en maintenant les dispositions relatives aux huit EC au niveau d'une norme. La majorité des exigences du cadre du PNS ont été promues au rang de pratiques recommandées, quelques-unes étant promues au rang de normes. Des indications détaillées sur les EC d'un système

SSO sont données dans le *Manuel de supervision de la sécurité*, Partie A — *Mise en place et gestion d'un système national de supervision de la sécurité* (Doc 9734).

8.2.2 Aperçu général d'un programme national de sécurité

8.2.2.1 Un PNS est un ensemble intégré de règlements et d'activités qui visent à améliorer la sécurité. Pour l'établissement et la tenue à jour du PNS, les SARP de l'OACI sont structurées selon les quatre composants suivants :

a) politique, objectifs et ressources 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.

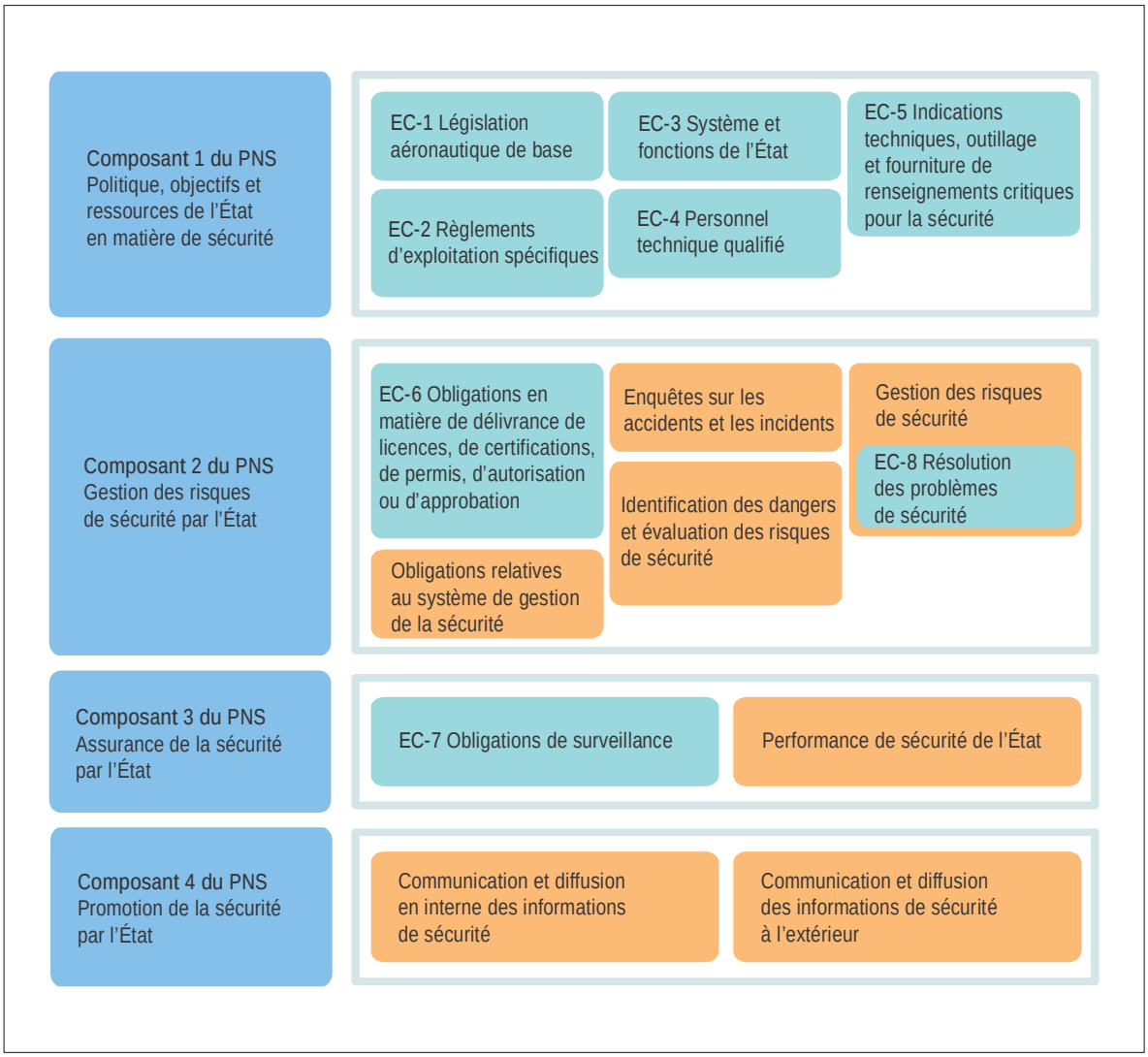

Figure 8-1. Programme national de sécurité intégré

8.2.2.2 La mise en œuvre d'un PNS exige une coordination entre les multiples autorités chargées des fonctions d'aviation de l'État. La mise en œuvre d'un PNS ne modifie en rien les rôles respectifs des organisations aéronautiques de l'État ou l'interaction normale entre elles. Au contraire, le PNS entend renforcer les fonctions et capacités collectives en matière de sécurité afin d'encore améliorer la sécurité au sein de l'État. Lorsqu'ils commencent à mettre en œuvre un PNS, la plupart des États découvrent qu'ils ont déjà des processus et activités en place qui abordent de nombreux aspects d'un PNS. La mise en œuvre d'un PNS vise à renforcer ces processus à l'aide d'éléments supplémentaires fondés sur le risque et relatifs à la performance et à la sécurité, et à faciliter la mise en œuvre effective d'un SGS par le secteur aéronautique de l'État.

8.2.2.3 Le PNS a pour objet :

a) d'assurer que l'État a mis en place un cadre législatif efficace avec, à l'appui, des règlements d'exploitation spécifiques ;

b) d'assurer une coordination et une synergie entre la GRS et l'assurance de la sécurité entre autorités aéronautiques nationales pertinentes ;

c) d'appuyer la mise en œuvre efficace et l'interaction appropriée avec les SGS des prestataires de services ;

d) de faciliter le suivi et la mesure de la performance de sécurité du secteur aéronautique de l'État ;

e) de maintenir et/ou de continuellement améliorer la performance de sécurité générale de l'État.

8.2.3 Délégation de fonctions et d'activités liées à la gestion de la sécurité

8.2.3.1 Certaines activités de gestion de la sécurité exigent de nouvelles compétences, telles que la réalisation d'évaluations des risques de sécurité, la réalisation d'analyses de données de sécurité ou l'évaluation de la pertinence de SPI.

8.2.3.2 Un État peut choisir de déléguer certaines fonctions ou tâches spécifiques découlant du PNS à un autre État, à une organisation régionale de supervision de la sécurité (RSOO) ou à une autre organisation compétente, telle qu'une association professionnelle, une organisation sectorielle représentative ou un organisme privé. Bien qu'un État puisse déléguer des fonctions spécifiques, il devra néanmoins disposer d'un personnel suffisant pour assurer l'interface avec l'entité à laquelle ces fonctions ont été déléguées et pour traiter les informations fournies par ladite entité.

8.2.3.3 Les États devraient aussi envisager de mettre en place des processus techniques et administratifs appropriés pour garantir que les fonctions déléguées soient assurées à leur entière satisfaction.

8.2.3.4 Quel que soit le type d'arrangement, l'État conserve la responsabilité de s'assurer que toute tâche déléguée soit exécutée conformément à ses exigences nationales et aux SARP.

8.2.3.5 La délégation peut permettre à des États ayant un niveau relativement faible d'activités aéronautiques de recueillir collectivement des données de sécurité pour identifier des tendances et coordonner des stratégies d'atténuation.

8.2.3.6 Si un État choisit de recevoir de l'aide pour l'élaboration de processus de surveillance, il devrait inclure l'élaboration de profils organisationnels de risque de sécurité pour les prestataires de services, la planification et la priorisation des inspections, les audits et activités de suivi d'organisations/prestataires de services approuvés.

8.2.3.7 Si un État choisit de déléguer les activités de surveillance, il devrait s'assurer qu'il conserve un accès aux dossiers de surveillance présentant des résultats documentés. L'État devrait aussi régulièrement surveiller et analyser la performance de sécurité de chaque prestataire de services et s'assurer qu'il est clairement établi qui surveillera et fera (le cas échéant) appliquer les mesures visant à résoudre tout problème de sécurité.

8.2.3.8 La délégation est un moyen pour les États ayant des ressources limitées de s'assurer qu'ils ont accès aux savoir-faire appropriés. Des orientations sur la mise en place d'une RSOO sont données dans le *Manuel de supervision de la sécurité,* Partie B — *Mise en place et gestion d'une organisation régionale de supervision de la sécurité* (Doc 9734).

8.3 COMPOSANT 1 : POLITIQUE, OBJECTIFS ET RESSOURCES DE L'ÉTAT EN MATIÈRE DE SÉCURITÉ

8.3.1 Le premier composant d'un PNS définit comment un État gérera la sécurité dans l'ensemble de son système d'aviation. Il inclut la détermination des exigences, obligations, fonctions et activités des différentes autorités aéronautiques de l'État qui sont liées au PNS ainsi que les grands objectifs de sécurité à atteindre. La politique et les objectifs de sécurité de l'État devraient être documentés pour exposer des attentes claires et veiller à ce que les efforts de gestion de la sécurité fournis par l'AAC de l'État et par d'autres autorités aéronautiques de l'État restent concentrés sur le maintien et l'amélioration de la performance de sécurité. Cela permet à l'État de donner des lignes directrices claires en matière de sécurité, à l'appui d'un système de transport aérien qui continue à croître et à se complexifier.

8.3.2 Le cadre juridique de l'État dicte les modalités de gestion de la sécurité de l'aviation. Les prestataires de services sont juridiquement responsables de la sécurité de leurs produits et services. Ils doivent se conformer aux réglementations en matière de sécurité établies par l'État. L'État devrait veiller à ce que les autorités aéronautiques concernées par la mise en œuvre et la tenue à jour du PNS aient les ressources nécessaires pour assurer une mise en œuvre efficace du PNS.

8.3.3 Le composant 1 du PNS, politique, objectifs et ressources de l'État en matière de sécurité, comprend les éléments suivants :

a) législation aéronautique de base ;

b) règlements d'exploitation spécifiques ;

c) système et fonctions de l'État ;

d) personnel technique qualifié ;

e) indications techniques, outillage et fourniture de renseignements critiques pour la sécurité.

8.3.4 Législation aéronautique de base

8.3.4.1 Des éléments indicatifs sur la législation aéronautique de base (EC-1) figurent dans le Doc 9734, Partie A.

Note.— Tout au long du présent manuel, le terme « législation » est employé dans son sens générique, de telle sorte qu'il englobe la législation aéronautique de base et les règlements d'exploitation spécifiques.

8.3.4.2 Il se peut qu'il faille des dispositions législatives qui habilitent les diverses autorités aéronautiques de l'État (p. ex. l'AAC ou le service d'enquête sur les accidents) à assumer leurs rôles. La législation aéronautique de base devra ou non mentionner spécifiquement la mise en œuvre du PNS comme rôle de l'AAC en fonction du système juridique de l'État. Certains États peuvent considérer que la mise en œuvre du PNS est implicite dans les fonctions déjà

mentionnées dans leur législation aéronautique de base. Dans ce cas, un amendement de la législation aéronautique de base ne sera peut-être pas nécessaire. Des preuves de la mise en œuvre d'un PNS devraient être clairement mentionnées dans des documents officiels de l'État. L'État devrait aussi pouvoir faire la preuve de son engagement à assumer ses responsabilités en matière de gestion de la sécurité, telles qu'exposées dans l'Annexe 19.

8.3.4.3 Dans le cadre de son PNS, l'État est tenu d'établir une politique d'application qui :

a) soutient et encourage une culture positive de la sécurité ;

b) décrit comment l'État assure la protection des données de sécurité et des informations de sécurité et de leurs sources connexes, surtout si les informations fournies sont auto-incriminantes ;

c) précise les conditions et circonstances dans lesquelles les prestataires de services ayant un SGS sont autorisés à traiter et à résoudre en interne des événements liés à certains problèmes de sécurité, dans les limites de leur SGS et à la satisfaction de l'autorité nationale pertinente, à condition que le SGS soit conforme au cadre pour un SGS et s'avère efficace et mature.

8.3.4.4 L'application des principes de gestion de la sécurité devrait amener la relation entre un État et ses prestataires de services à dépasser le stade de la conformité et de l'exécution pour évoluer en un partenariat visant à maintenir ou à améliorer continuellement la performance de sécurité.

8.3.5 Règlements d'exploitation spécifiques

8.3.5.1 Des éléments indicatifs sur les règlements d'exploitation spécifiques (EC-2), y compris l'adaptation ou l'adoption de réglementations d'un autre État, figurent dans le Doc 9734, Partie A.

Réglementations normatives et réglementations fondées sur les performances

8.3.5.2 Les réglementations en matière de sécurité constituent un outil important qui peut être utilisé par les États pour maîtriser les risques de sécurité. La transition vers la gestion de la sécurité a aussi généré une tendance à introduire des réglementations fondées sur les performances. Pour comprendre ce que sont ces réglementations fondées sur les performances, il faut tout d'abord comprendre les réglementations normatives. Les réglementations normatives sont des réglementations qui énoncent explicitement ce qui doit être fait et comment il faut le faire. On s'attend à ce que le respect de ces réglementations permette d'atteindre le niveau souhaité de sécurité. Beaucoup de réglementations normatives ont été élaborées après un accident et reposent sur les leçons tirées et sur le désir d'éviter qu'à l'avenir un accident soit dû à des causes identiques. Du point de vue du prestataire de services, le respect des exigences normatives implique la mise en œuvre de ces réglementations sans le moindre écart. Aucune analyse ou justification supplémentaire n'est attendue du prestataire de services ou de l'autorité.

8.3.5.3 Jusqu'il y a peu, les SARP de l'OACI se concentraient sur des exigences normatives en tant que moyen d'identifier les normes minimums et de garantir l'interopérabilité. Toutefois, on voit apparaître de plus en plus un besoin de permettre à des réglementations fondées sur les performances de soutenir des approches novatrices de la mise en œuvre qui sont susceptibles d'améliorer l'efficacité et d'atteindre ou de dépasser les objectifs de sécurité.

8.3.5.4 Les Annexes de l'OACI donnent des exemples de normes qui permettent des réglementations normatives et des réglementations fondées sur les performances. Voici un exemple de norme de l'Annexe 14 — *Aérodromes,* Volume I — *Conception et exploitation technique des aérodromes*, qui permet des réglementations normatives :

> *3.3.1 Une aire de demi-tour sera aménagée aux extrémités des pistes qui ne sont pas desservies par une voie de circulation ou par une voie de demi-tour et où la lettre de code est D, E ou F, afin de faciliter l'exécution de virages à 180°.*

8.3.5.5 L'exemple précité permet une réglementation normative car il identifie une seule manière de se mettre en conformité si la piste répond aux critères spécifiés, à savoir fournir une aire de demi-tour. Des écarts par rapport aux réglementations normatives sont généralement accordés au moyen de dérogations aux réglementations.

8.3.5.6 Par contre, les normes qui permettent des réglementations fondées sur les performances sont exprimées en termes de résultat souhaité. Les réglementations fondées sur les performances qui en résultent exigent que les prestataires de services prouvent que leur approche proposée atteindra le résultat souhaité. Voici un exemple de norme fondée sur les performances, tiré de l'Annexe 6, Partie 1.

> *7.2.11 Tout avion sera doté d'un équipement de navigation suffisant pour que, si un élément de l'équipement tombe en panne à un moment quelconque du vol, le reste de l'équipement permette de naviguer conformément aux dispositions du § 7.2.1 et, le cas échéant, à celles des § 7.2.2, 7.2.5 et 7.2.6.*

8.3.5.7 Il convient de noter que la norme ci-dessus n'indique pas l'équipement de navigation spécifique requis. Elle décrit au contraire le résultat souhaité, à savoir qu'en cas de défaillance d'un élément, le reste de l'équipement doit permettre de continuer à assurer une conduite sûre de l'aéronef. L'équipement requis dépendra de la conception de l'aéronef. Les réglementations rédigées de cette manière exigeraient de l'exploitant aérien qu'il fournisse à l'autorité les données nécessaires pour montrer comment il respecte cette exigence. Il peut le faire par sa propre analyse mais pour ce type de réglementations fondées sur les performances, les informations requises sont souvent disponibles auprès d'autres sources. Dans ce cas, tant l'autorité que l'exploitant aérien utiliseraient les données des constructeurs d'aéronefs pour les guider dans leur décision et il n'est nullement nécessaire que l'exploitant aérien élabore sa propre solution inédite. Lorsqu'ils élaborent des réglementations fondées sur les performances, les États doivent garder à l'esprit comment la conformité à ces réglementations pourra être prouvée. Il se peut que les États doivent élaborer des éléments indicatifs et/ou des moyens acceptables de mise en conformité pour aider le secteur à satisfaire à l'exigence.

8.3.5.8 Voici un autre exemple de norme fondée sur les performances, tiré de l'Appendice 2 à l'Annexe 19.

> *2.1.1 Le prestataire de services élaborera et tiendra à jour un processus pour déterminer les dangers liés à ses produits ou services aéronautiques.*

8.3.5.9 Dans l'exemple ci-dessus, bien que la norme exige qu'un processus soit mis en place pour déterminer les dangers, elle ne spécifie pas quel doit être ce processus. Les États peuvent autoriser les prestataires de services à concevoir leur propre méthodologie. Le rôle de l'autorité de réglementation serait d'évaluer si la méthodologie, les processus et le système du prestataire de services aboutiraient effectivement à la détermination des dangers. L'autorité évaluerait aussi la performance du processus d'identification des dangers du prestataire de services, par exemple en évaluant le volume, les types et l'importance des dangers identifiés. Les réglementations fondées sur les performances qui sont formulées de cette manière exigent des autorités de réglementation qu'elles aient les compétences et les savoir-faire requis pour évaluer la performance du système, plutôt que de simplement évaluer une conformité à la lettre à des réglementations normatives. Il faudra aussi plus de ressources pour l'évaluation car la mise en œuvre variera d'un prestataire de services à l'autre.

Proposer des options normatives et fondées sur les performances

8.3.5.10 Dans certains cas, les SARP de l'OACI exigent l'adoption de réglementations normatives tout en offrant aux États la possibilité de choisir l'instauration de réglementations fondées sur les performances à l'appui d'autres moyens de mise en conformité. Lorsque des États mettent en place à la fois des réglementations normatives et des options réglementaires fondées sur les performances, les prestataires de services qui n'ont pas les savoir-faire requis pour élaborer leur propre approche en vue de se conformer aux réglementations fondées sur les performances peuvent choisir de respecter les réglementations normatives. Par contre, ce choix de réglementations permet aux prestataires de services qui ont les savoir-faire requis d'élaborer un moyen de mise en conformité qui soit approprié à leurs propres opérations et peut aussi offrir la possibilité d'accroître la flexibilité opérationnelle et l'utilisation plus efficace des ressources. Les normes de

gestion de la fatigue, telles que celles qui figurent dans l'Annexe 6, Partie 1, à l'Amendement n° 43, en livrent un bon exemple :

> *4.10.1 L'État de l'exploitant établira des règlements aux fins de la gestion de la fatigue. Ces règlements seront fondés sur des principes scientifiques, des connaissances et l'expérience opérationnelle, le but étant de garantir que les membres des équipages de conduite et de cabine s'acquittent de leurs fonctions avec un niveau de vigilance satisfaisant. L'État de l'exploitant établira donc :*
>
> *a) des règles normatives concernant des limites de vol, de période de service de vol, de période de service ainsi que des exigences en matière de repos ;*
>
> *b) s'il autorise des exploitants à utiliser un système de gestion des risques de fatigue (FRMS) pour gérer la fatigue, des règlements applicables à un tel système.*
>
> *4.10.2 L'État de l'exploitant exigera que l'exploitant établisse, en application du § 4.10.1 et aux fins de la gestion des risques de sécurité liés à la fatigue :*
>
> *a) des limites de temps de vol, de période de service de vol et de période de service ainsi que des exigences en matière de repos qui respectent les règles normatives de gestion de la fatigue établies par l'État de l'exploitant ; ou*
>
> *b) un système de gestion des risques de fatigue (FRMS) pour l'ensemble de ses activités compte tenu des dispositions du § 4.10.6 ; ou*
>
> *c) un FRMS pour une partie de ses activités compte tenu des dispositions du § 4.10.6, et les limites prévues au § 4.10.2, alinéa a), pour le reste de ses activités.*

8.3.5.11 Dans l'exemple ci-dessus, la norme exige que les États établissent des règles normatives de limitation du temps de vol et des périodes de service, tandis que l'instauration de règles à l'appui d'un FRMS est facultative. Le FRMS donne à l'exploitant aérien l'occasion de mieux gérer les risques spécifiques liés à la fatigue tout en lui offrant la possibilité de mettre en place une flexibilité opérationnelle en dehors des règles normatives régissant la limitation des temps de vol et des périodes de service. Les États doivent envisager s'il est nécessaire de prévoir, en variante, des règles du FRMS en plus des limitations normatives obligatoires et doivent estimer s'ils ont les ressources nécessaires pour assurer une supervision appropriée du FRMS. La norme 4.10.2 précise ensuite que les exploitants aériens doivent gérer leurs risques de sécurité liés à la fatigue. Lorsque des règles sont établies pour le FRMS, ils peuvent le faire dans les limites normatives mentionnées au § 4.10.2, alinéa a), ou en mettant en œuvre un FRMS fondé sur les performances, tel qu'évoqué au § 4.10.2, alinéas b) et c). Les exploitants aériens qui n'ont pas le savoir-faire requis pour élaborer un FRMS et respecter les exigences réglementaires qui y sont liées devront se conformer aux réglementations normatives.

8.3.5.12 Il devrait être manifeste que les réglementations fondées sur les performances ne sont pas toujours appropriées. Les exigences normatives restent appropriées lorsqu'un moyen normalisé de mise en conformité est requis, par exemple pour faciliter l'interopérabilité. Les exigences relatives aux marques des pistes, par exemple, sont nécessairement de nature normative.

8.3.5.13 Dans la pratique, les réglementations sont rarement totalement normatives ou totalement fondées sur les performances ; elles contiennent plutôt des éléments des deux types. Elles sont aussi fondées sur les performances à des degrés divers. Lorsqu'un État envisage de mettre en œuvre des réglementations fondées sur les performances, il doit tenir compte de la capacité et de la maturité du secteur, de sous-secteurs spécifiques, voire de la maturité des divers prestataires de services et de leurs SGS. Les réglementations fondées sur les performances exigent en outre une plus grande intervention de l'autorité de réglementation, celle-ci devant non seulement vérifier la conformité mais aussi être à même d'évaluer des systèmes et la performance de sécurité en tenant compte du contexte opérationnel

spécifique de chaque prestataire de services. Les États doivent veiller à être en mesure de continuer à superviser et à gérer le secteur, en sachant que cela exigera plus de savoir-faire et de ressources. Les SGS donnent aux prestataires de services une base et des outils pour satisfaire aux réglementations fondées sur les performances mais on ne peut pas avoir automatiquement la certitude que chaque prestataire de services ayant un SGS pourra se conformer à ces réglementations. Tout dépend de ce que requièrent les exigences spécifiques fondées sur les performances.

8.3.5.14 Les réglementations fondées sur les performances influent aussi sur l'application des règles. L'application des règles normatives est simple car il est aisé d'établir la non-conformité. L'application des réglementations fondées sur les performances est plus difficile. Par exemple, un prestataire de services peut être capable de montrer qu'il a mis en place un processus qui respecte la réglementation (p. ex. un système de compte rendu de dangers), mais il ne peut démontrer que ce processus est à même de livrer le résultat escompté (p. ex. prouver que le système de compte rendu de dangers est efficace). Cela pourrait mener à la mise en place de systèmes ou de processus qui satisfont uniquement à la « lettre de la loi », sans livrer le résultat de sécurité requis. Les autorités de réglementation devront peut-être associer les services pertinents d'application de la loi à l'élaboration de réglementations fondées sur les performances afin de garantir leur caractère exécutoire.

8.3.6 Système et fonctions de l'État

8.3.6.1 Des éléments indicatifs sur le système et les fonctions de l'État (EC-3) figurent dans le Doc 9734, Partie A.

Organisation responsable de la coordination du PNS

8.3.6.2 Les responsabilités de l'État en matière de gestion de la sécurité peuvent être assumées par de multiples autorités de l'aviation au sein de l'État, notamment l'AAC et un AIA indépendants. Les États devraient clarifier quelle autorité au sein de l'État est chargée de coordonner la tenue à jour et la mise en œuvre du PNS. De nombreux États attribuent ce rôle à l'AAC, étant donné que l'AAC doit normalement assumer la plupart des responsabilités du PNS. Les rôles et responsabilités de toutes les autorités concernées devraient être identifiés et documentés.

Groupe de coordination du PNS

8.3.6.3 L'État devrait créer un groupe de coordination approprié comptant des représentants des autorités de l'aviation concernées ayant des responsabilités en matière de mise en œuvre et de tenue à jour du PNS, y compris des services d'enquête sur les accidents ainsi que des autorités de l'aviation militaire. La désignation d'un groupe de coordination facilitera une bonne communication, évitera les chevauchements d'efforts et des politiques contradictoires et garantira une mise en œuvre efficace et efficiente du PNS. Ce groupe est une forme de comité présidé par le directeur de l'organisation responsable de la coordination du PNS.

8.3.6.4 L'État peut aussi estimer bénéfique d'attribuer la planification et la gestion quotidiennes de la mise en œuvre du PNS à une personne, un département ou une équipe. De tels personne, département ou équipe peuvent veiller à une bonne corrélation entre les différents aspects du travail en vue d'atteindre les objectifs de sécurité de l'État.

Fonctions et activités du PNS

8.3.6.5 Il appartient à chaque État de décider comment il structure son personnel et ses organisations en vue d'assurer l'acceptation et le suivi de la mise en œuvre des SGS par les prestataires de services, conformément à l'Annexe 19. Un État peut décider de créer un nouveau bureau ou d'ajouter cette responsabilité aux responsabilités des bureaux existants, par exemple, le bureau de la navigabilité, le bureau de l'exploitation technique, le bureau de la navigation aérienne et le bureau des aérodromes, etc. La décision dépendra de la façon dont l'État choisit de satisfaire aux nouvelles exigences en matière de compétences.

8.3.6.6 Il est important pour les diverses autorités de l'aviation de clarifier les rôles. Dans ces rôles, elles devraient inclure toutes leurs obligations, fonctions et activités découlant du PNS. L'État devrait s'assurer que chaque autorité comprend quel rôle elle doit jouer pour réaliser chacune des exigences de l'Annexe 19 et, point le plus important, quelle est sa responsabilité dans la gestion de la sécurité au sein de l'État. Les obligations et fonctions de chaque autorité de l'aviation en ce qui concerne la mise en œuvre du PNS devraient être documentées afin d'éviter toute ambiguïté.

8.3.6.7 Les États dont le personnel affecté à la sécurité est géographiquement dispersé devraient se doter de structures de gouvernance appropriées. Une structure de gouvernance complexe n'est peut-être pas nécessaire pour des systèmes d'aviation moins complexes, où peu de personnes participent à la gestion de la sécurité. L'État devrait s'assurer que tout le personnel a la même compréhension de la mise en œuvre du PNS au niveau national. L'approche de la mise en œuvre du PNS devrait être documentée.

Politique et objectifs de sécurité de l'État

8.3.6.8 Une mise en œuvre efficace d'un PNS exige un engagement des hauts responsables de l'État et l'appui du personnel à tous les échelons. Les politiques et objectifs de sécurité d'un État sont des déclarations de haut niveau approuvées par les autorités de l'aviation de l'État. Ensemble, ils guident les comportements en matière de sécurité et l'affectation des ressources à la sécurité. La politique et les objectifs de sécurité de l'État devraient être publiés et réexaminés périodiquement pour s'assurer qu'ils demeurent pertinents et qu'ils conviennent en permanence à l'État.

Politique de sécurité de l'État

8.3.6.9 L'engagement des hauts responsables devrait être explicite dans la politique de sécurité de l'État. La politique de sécurité de l'État est un document formel qui décrit les intentions et la direction adoptées par l'État en matière de sécurité. La politique de sécurité de l'État traduit l'attitude des hauts responsables envers la sécurité et envers la promotion d'une culture positive de la sécurité dans l'État. On peut la concevoir comme l'énoncé de mission et de vision de l'État en ce qui concerne la sécurité.

8.3.6.10 La politique de sécurité devrait aborder les pratiques clés qui sont essentielles pour la gestion de la sécurité et la façon dont les hauts responsables espèrent assumer leurs responsabilités en matière de sécurité (p. ex. utilisation d'une approche fondée sur les données). Les principes reflétés dans la politique de sécurité devraient être clairement visibles dans les pratiques quotidiennes de l'État.

8.3.6.11 La politique de sécurité de l'État est approuvée par les autorités de l'aviation de l'État, qui prouvent ainsi leurs intentions en matière de sécurité, et est mise en œuvre en tant que procédure ou protocole. Voici un énoncé de politique type : « Nous réaliserons la sécurité par : 1) notre acceptation des obligations de rendre compte des conditions et comportements sûrs ; 2) une culture de leadership, de collaboration, de communication ouverte, etc., en matière de sécurité. »

Objectifs de sécurité de l'État

8.3.6.12 L'élaboration d'objectifs de sécurité commence par une compréhension claire des risques de sécurité les plus élevés dans le système aéronautique. Les risques de sécurité dans le système aéronautique sont influencés par de nombreux facteurs, tels que la taille et la complexité du système aéronautique ainsi que l'environnement d'exploitation. L'élaboration d'une bonne description du système assurera un contexte et une compréhension corrects. Voir le § 8.7 du présent chapitre sur la mise en œuvre du PNS.

8.3.6.13 Lorsqu'elles sont disponibles, des données quantitatives devraient être utilisées pour acquérir une compréhension des risques de sécurité principaux. L'État peut aussi utiliser des informations qualitatives et des analyses d'experts. Un groupe d'experts sélectionnés peut être créé pour participer à des discussions dirigées afin de

mieux comprendre les grands risques de sécurité dans l'ensemble du système aéronautique. Ce groupe aurait un rôle similaire à celui de la commission d'examen de la sécurité (SRB) du prestataire de services, présentée au Chapitre 9, § 9.3.6, mais dans ce cas, au niveau de l'État. Ces experts peuvent être guidés par les informations disponibles sur les tendances en matière de sécurité, sur les facteurs contributifs connus à des accidents et incidents graves, ou sur les lacunes connues dans les processus SSO de l'État. Ils pourraient aussi envisager des objectifs régionaux ou des objectifs mondiaux, tels qu'identifiés dans le GASP. Cette approche de type recherche d'idées pourrait être menée en collaboration avec des prestataires de services, afin d'identifier les problèmes de sécurité « connus » pour chaque secteur de l'aviation.

8.3.6.14 Les objectifs de sécurité de l'État sont de brefs énoncés de haut niveau qui donnent une orientation pour toutes les autorités pertinentes en charge de l'aviation au sein de l'État. Ils représentent les résultats souhaités en matière de sécurité que l'État entend atteindre. Il importe aussi, lorsque l'on définit les objectifs de sécurité, de tenir compte de la capacité de l'État à influencer les résultats souhaités. Les objectifs de sécurité représentent les priorités de l'État pour la gestion de la sécurité et offrent une base pour la répartition et l'affectation des ressources de l'État.

8.3.6.15 Les objectifs de sécurité soutiennent l'identification des SPI et des SPT de l'État et l'établissement subséquent du niveau acceptable de performance de sécurité (ALoSP), qui sera examiné plus loin dans le présent chapitre. Les objectifs de sécurité constituent un ensemble avec les SPI et les SPT pour permettre à l'État d'assurer le suivi et la mesure de sa performance de sécurité. Le Chapitre 4 contient de plus amples indications sur les SPI et les SPT.

8.3.6.16 Une fois le PNS mis en œuvre, l'État devrait régulièrement réévaluer ses risques de sécurité identifiés, en analysant les informations de sécurité générées par le PNS. L'analyse soutiendra aussi l'identification des problèmes émergents. De plus amples informations sur l'analyse de sécurité figurent au Chapitre 6. L'État devrait aussi analyser régulièrement ses progrès sur la voie de la réalisation de ses objectifs de sécurité et évaluer si ceux-ci restent pertinents, en gardant à l'esprit toute réévaluation des risques actuels.

Ressources affectées par l'État à la sécurité

8.3.6.17 L'État doit s'assurer que les agences qui ont des responsabilités en matière de sécurité reçoivent des ressources suffisantes pour s'acquitter de leurs mandats. Les ressources concernées sont à la fois financières et humaines.

8.3.6.18 Certaines autorités de l'aviation reçoivent leurs financements sur la base d'un budget affecté par l'État. D'autres sont financées par des redevances et charges perçues auprès de ceux qui participent au système aéronautique (telles que les redevances pour l'obtention d'une licence ou d'une approbation) ou auprès des usagers de services du système aéronautique (p. ex. des redevances sur les passagers ou le carburant). La source de financement la plus appropriée pour l'État dépend des circonstances de l'État en question. Par exemple, un État qui a un petit secteur aéronautique peut estimer que son AAC ne peut s'appuyer uniquement sur les redevances et charges pour financer ses activités de réglementation. Il est possible qu'un État doive avoir des sources de financement multiples pour ses activités aéronautiques.

8.3.6.19 Lorsque des États commencent à pleinement mettre en œuvre leur PNS et à adopter des pratiques de gestion de la sécurité, il est possible qu'ils doivent revoir leur budget et leur financement pour garantir qu'ils continuent à avoir un flux suffisant de recettes. De nouvelles fonctions sont introduites (notamment la GRS, la collecte et l'analyse de données et la promotion de la sécurité) et doivent être bien exécutées pour qu'une approche de la gestion de la sécurité soit couronnée de succès. La gestion de la sécurité exige en outre que les autorités de l'aviation de l'État soient capables de surveiller et analyser en permanence leurs propres processus pour gérer le risque. Des inspecteurs et d'autres membres du personnel pourraient devoir suivre des recyclages. L'État pourrait estimer nécessaire d'affecter des ressources financières suffisantes aux agences de l'État qui entament une transition vers une approche de la gestion de la sécurité.

Plan national pour la sécurité de l'aviation (NASP)

8.3.6.20 La Résolution A39-12 de l'Assemblée sur la planification mondiale de l'OACI en matière de sécurité et de navigation aérienne reconnaît l'importance d'une mise en œuvre effective des plans nationaux pour la sécurité de l'aviation. Elle décide que les États doivent élaborer et mettre en œuvre des plans nationaux pour la sécurité de l'aviation, conformes aux buts du Plan pour la sécurité de l'aviation dans le monde (GASP, Doc 10004). Au niveau international, le GASP énonce une stratégie qui soutient la priorisation et l'amélioration continue de la sécurité de l'aviation. Des plans régionaux et nationaux pour la sécurité de l'aviation devraient être élaborés conformément au GASP.

8.3.6.21 Au niveau régional, les groupes régionaux de sécurité de l'aviation (RASG) coordonnent le processus de planification. Les initiatives régionales et nationales de renforcement de la sécurité (SEI) devraient être adaptées sur la base des problèmes auxquels les États concernés sont confrontés. Le plan national pour la sécurité de l'aviation présente l'orientation stratégique pour la gestion de la sécurité de l'aviation au niveau national, pour une durée déterminée (p. ex. pour les cinq prochaines années). Il expose à toutes les parties prenantes à quoi les autorités nationales de l'aviation devraient affecter les ressources durant les années à venir.

8.3.6.22 Un plan national pour la sécurité de l'aviation permet à l'État de communiquer clairement sa stratégie pour améliorer la sécurité au niveau national à toutes les parties prenantes, y compris à d'autres organismes gouvernementaux et aux voyageurs. Il constitue un moyen transparent pour expliquer comment les AAC et d'autres entités actives dans l'aviation civile collaboreront pour identifier les dangers et gérer les risques pour la sécurité de l'exploitation et d'autres problèmes de sécurité. Il illustre en outre comment les SEI planifiées aideront l'État à atteindre les buts fixés. Le plan national pour la sécurité de l'aviation souligne l'engagement de l'État à assurer la sécurité de l'aviation.

8.3.6.23 Chaque État devrait publier un plan national pour la sécurité de l'aviation. Si un État a déjà mis en place un PNS, le plan national pour la sécurité de l'aviation peut être abordé par le composant 1 : politique, objectifs et ressources de l'État en matière de sécurité. Le plan national pour la sécurité de l'aviation peut être publié en tant que document de haut niveau distinct, afin de faciliter la communication avec le public et avec d'autres entités externes à l'AAC.

Documentation du PNS

8.3.6.24 L'État devrait décrire son PNS dans un document afin de garantir que tous les membres du personnel concernés en aient une compréhension commune. Ce document devrait inclure la structure du PNS et les programmes qui y sont associés, comment les divers composants interagissent ainsi que les rôles des différentes autorités aéronautiques de l'État. Cette documentation devrait compléter les processus et procédures existants et décrire dans les grandes lignes comment les divers sous-programmes du PNS fonctionnent ensemble aux fins d'améliorer la sécurité. On peut aussi ajouter des références croisées aux responsabilités et obligations redditionnelles des autorités dans des documents d'appui. L'État devrait choisir un moyen de documentation et de diffusion qui servirait au mieux son environnement, par exemple un document physique ou un site web doté des contrôles appropriés. Quel que soit le canal de communication, le but est de faciliter une compréhension commune du PNS par tous les membres du personnel concernés.

8.3.7 Personnel technique qualifié

8.3.7.1 Des éléments indicatifs sur le personnel technique qualifié assumant des fonctions liées à la sécurité (EC-4) figurent dans le Doc 9734, Partie A.

Éléments indicatifs généraux

8.3.7.2 Les États devront identifier et gérer les compétences requises pour une mise en œuvre effective du PNS, en tenant compte des rôles et responsabilités découlant du PNS qui sont assurés par leur personnel. Ces compétences viennent s'ajouter à celles qui sont requises pour la réalisation de la supervision de la conformité et peuvent être gérées

par la formation du personnel existant ou l'embauche de collaborateurs supplémentaires et incluent, mais sans s'y limiter :

a) des compétences de leadership accrues ;

b) la compréhension des processus commerciaux ;

c) l'expérience et le discernement requis pour évaluer la performance et l'efficacité ;

d) la surveillance fondée sur le risque de sécurité ;

e) la collecte et l'analyse des données de sécurité ;

f) la mesure et le suivi de la performance de sécurité ;

g) les activités de promotion de la sécurité.

8.3.7.3 Des orientations sur la création et le maintien de solides équipes d'inspection figurent dans le *Manual on the Competencies of Civil Aviation Safety Inspectors* (Manuel sur les compétences des inspecteurs de la sécurité de l'aviation civile) (Doc 10070).

8.3.7.4 L'État devrait déterminer la formation la plus appropriée pour le personnel assumant différents rôles et responsabilités au sein de l'organisation. Voici des exemples de formations qui devraient être envisagées :

a) briefings ou formation de familiarisation sur le PNS, les SGS, la politique de sécurité, les objectifs et l'ALoSP, destinés aux hauts responsables ;

b) formation pour les inspecteurs sur les principes du PNS et des SGS, sur la façon de mener des évaluations des SGS, sur la façon d'évaluer les SPI d'un prestataire de services en vue de leur acceptation, et sur la façon de mener une supervision générale du prestataire de services dans un environnement de gestion de la sécurité ;

c) formation aux compétences non techniques (aptitudes en matière de communication efficace, aptitudes à la négociation, aptitudes dans le domaine de la résolution des conflits, etc.) pour aider les inspecteurs à collaborer avec les prestataires de services en vue d'améliorer la performance de sécurité tout en assurant un respect en continu des réglementations établies ;

d) formation pour le personnel chargé de l'analyse des données, des objectifs de sécurité, des SPI et des SPT ;

e) formation pour les médecins-examinateurs et les évaluateurs médicaux de l'aviation ;

f) protection des données de sécurité, des informations de sécurité et des sources connexes et formation à une politique d'application des réglementations pour le personnel juridique, etc. ;

g) formation au PNS et au SGS pour les enquêteurs de la sécurité des prestataires de services.

8.3.7.5 Les programmes de formation à la sécurité destinés aux membres du personnel associés à des tâches liées au PNS devraient être coordonnés entre organisations de l'État, selon le cas. La portée de la formation ou de la familiarisation au PNS et au SGS devrait refléter les processus réels du PNS, et le PNS lui-même à mesure que celui-ci évolue et mûrit. La formation initiale au PNS et au SGS peut être limitée à des éléments génériques du PNS ou à des éléments et orientations-cadres du SGS.

8.3.7.6 Pour garantir que tout le personnel technique pertinent ait les qualifications appropriées, l'État devrait :

a) élaborer des politiques et procédures de formation internes ;

b) élaborer un programme de formation au PNS et au SGS pour le personnel pertinent. La priorité devrait être donnée au personnel affecté à la mise en œuvre du PNS-SGS et aux inspecteurs d'exploitation/de terrain participant à la surveillance/au suivi du SGS des prestataires de services (y compris des processus du PNS spécifiques à l'État et de leur pertinence).

8.3.7.7 Beaucoup de types de formations au PNS et au SGS sont disponibles, y compris des cours en ligne, des cours en classe, des ateliers, etc. Le type et le volume de formation fournis devraient garantir que le personnel pertinent acquière les compétences requises pour assumer ses rôles et pour comprendre sa contribution au PNS. Le but est de garantir que les personnes ou les équipes abordent chaque aspect du PNS et soient formées pour assumer le rôle qui leur a été imparti.

8.3.7.8 Une formation appropriée et suffisante pour les inspecteurs garantira une surveillance cohérente et leur donnera les capacités requises pour être efficaces dans un environnement de gestion de la sécurité. Les États devraient envisager les aspects suivants :

a) La surveillance et le suivi des SGS des prestataires de services exigeront des compétences qui pourraient ne pas avoir été cruciales avant l'introduction des exigences relatives aux SGS. Les inspecteurs devront compléter leurs connaissances techniques existantes par des aptitudes supplémentaires pour évaluer si la mise en œuvre des SGS des prestataires de services est appropriée et effective. Cette approche exige un travail en partenariat avec l'industrie afin de gagner la confiance des prestataires de services pour faciliter le partage des données de sécurité et des informations de sécurité. Les États devront fournir la formation appropriée pour garantir que le personnel chargé de l'interaction avec l'industrie ait les compétences et la flexibilité requises pour assurer des activités de surveillance dans un environnement de SGS. Une analyse des besoins de formation peut être utilisée pour identifier les formations appropriées.

b) La formation devrait aussi donner au personnel une conscience du rôle et des contributions des autres services au sein de leur autorité de l'aviation et des autorités de l'aviation d'autres États. Cela permettra aux inspecteurs ainsi qu'au personnel de différentes autorités nationales de l'aviation d'adopter une approche cohérente. Cela facilitera en outre une meilleure compréhension des risques de sécurité dans divers secteurs. Les inspecteurs pourront aussi mieux comprendre comment ils contribuent à la réalisation des objectifs de sécurité de l'État.

8.3.8 Indications techniques, outillage et fourniture de renseignements critiques pour la sécurité

8.3.8.1 Des éléments indicatifs sur les indications techniques, l'outillage et la fourniture de renseignements critiques pour la sécurité (EC-5) figurent dans le Doc 9734, Partie A.

8.3.8.2 L'État devrait envisager de donner des orientations à ses inspecteurs et à ses prestataires de services pour les aider dans l'interprétation des réglementations relatives à la gestion de la sécurité. Il encouragera ainsi une culture positive de la sécurité et aidera les prestataires de services à atteindre leurs objectifs de sécurité et, en conséquence, les objectifs de sécurité de l'État, souvent réalisés par le biais de réglementations. L'évaluation des SGS peut requérir des outils supplémentaires permettant d'établir à la fois la conformité et la performance des SGS des prestataires de services. Tout outil élaboré nécessitera une formation du personnel affecté à son utilisation, avant la mise en œuvre.

8.4 COMPOSANT 2 : GESTION DES RISQUES DE SÉCURITÉ PAR L'ÉTAT

8.4.1 Les États doivent identifier les risques de sécurité potentiels pour le système aéronautique. À cette fin, ils devraient renforcer leurs méthodes traditionnelles d'analyse des causes d'accidents ou d'incidents par des processus proactifs. Les processus proactifs permettent aux États d'identifier et de traiter les signes précurseurs d'accidents et les facteurs contributifs et d'appliquer une gestion stratégique des ressources affectées à la sécurité afin de maximiser les améliorations de la sécurité. Les États devraient :

a) exiger que leurs prestataires de services mettent en œuvre un SGS pour gérer et améliorer la sécurité de leurs activités liées à l'aviation ;

b) établir des moyens de déterminer si la GRS des prestataires de services est acceptable ;

c) procéder à un réexamen afin de s'assurer que le SGS du prestataire de services reste efficace.

8.4.2 Le composant GRS de l'État inclut la mise en œuvre de SGS par les prestataires de services, y compris de processus d'identification des dangers et de gestion des risques de sécurité qui y sont associés.

8.4.3 Les États devraient aussi appliquer les principes de la GRS à leurs propres activités, notamment à l'élaboration de réglementations et à l'établissement des priorités pour les activités de surveillance fondées sur les risques évalués.

8.4.4 Un domaine souvent négligé par les prestataires de services et par les autorités de réglementation est le risque de sécurité induit par les interfaces avec d'autres entités. L'interface entre le PNS et le ou les SGS peut poser un défi particulier aux États et aux prestataires de services. L'État devrait envisager de souligner l'importance de la gestion du risque aux interfaces du SGS par le biais de ses réglementations et de ses orientations d'appui. Voici des exemples de risques aux interfaces :

a) Dépendance — l'organisation A dépend de l'organisation B pour fournir des biens ou services. L'organisation B ne connaît pas clairement les attentes ni la dépendance de l'organisation A et ne livre pas les résultats escomptés.

b) Contrôle — les organisations en interface exercent souvent un contrôle minimal de la qualité ou de l'efficacité de la ou des organisations avec lesquelles elles sont en interface.

8.4.5 Dans ces deux cas, la gestion des risques aux interfaces peut mettre en lumière le risque, clarifier les attentes mutuelles et atténuer les conséquences indésirables par l'instauration de vérifications convenues d'un commun accord aux interfaces. De plus amples informations sur les interfaces entre prestataires de services figurent au Chapitre 2.

8.4.6 Obligations en matière de délivrance de licences, de certifications, de permis, d'autorisation ou d'approbation

8.4.6.1 Des éléments indicatifs sur les obligations en matière de délivrance de licences, de certifications, de permis, d'autorisation ou d'approbation (EC-6) figurent dans le Doc 9734, Partie A.

8.4.6.2 Les obligations en matière de délivrance de licences, de certifications, de permis, d'autorisation ou d'approbation sont des composants importants de la stratégie de l'État en matière de maîtrise des risques de sécurité. Elles donnent à l'État l'assurance que les prestataires de services et d'autres organisations pertinentes, représentatives du secteur, ont atteint les normes requises pour assurer une exploitation sûre au sein du système aéronautique. Certains États ont établi des règlements d'exploitation communs pour faciliter la reconnaissance ou l'acceptation de licences, certificats, autorisations et approbations délivrés par d'autres États. De tels arrangements n'exonèrent pas les États de leurs obligations en vertu de la Convention de Chicago.

8.4.7 Obligations relatives au système de gestion de la sécurité

Exigences réglementaires relatives au SGS

8.4.7.1 Conformément à l'Annexe 19, l'État doit exiger que les prestataires de services et les exploitants de l'aviation générale internationale mettent en œuvre un SGS. Les exigences portent sur le cadre pour un SGS figurant à l'Appendice 2 de l'Annexe 19 et sur les orientations d'appui présentées au Chapitre 9 du présent manuel. Les modalités d'établissement de ces exigences dépendront du cadre réglementaire de l'État.

8.4.7.2 Les États devraient instituer un processus qui garantisse que le SGS soit acceptable pour l'État. Une approche consiste à établir, au niveau de l'État, des calendriers et des échéances qui représentent les progrès requis dans la mise en œuvre du SGS. Des orientations supplémentaires pour les prestataires de services sur la façon d'élaborer et d'exécuter une analyse des lacunes et un plan de mise en œuvre du SGS figurent au Chapitre 9.

8.4.7.3 L'État devrait réévaluer périodiquement ses exigences réglementaires relatives au SGS et ses documents d'orientation sur le SGS. Cet examen devrait prendre en considération les rétro-informations de l'industrie, l'analyse périodique du profil de risque de sécurité de l'État, la situation actuelle et l'applicabilité des SARP et des orientations de l'OACI relatives aux SGS.

Aviation générale internationale

8.4.7.4 Les dispositions des SGS relatives à l'aviation générale internationale (AGI) sont abordées avec une certaine flexibilité dans l'Annexe 19 et ne sont dès lors pas reprises dans la liste des prestataires de services. Ce secteur de l'aviation est tenu de mettre en œuvre le cadre pour un SGS. Toutefois, à la différence d'autres secteurs, il bénéficie de la possibilité accordée aux États de faire preuve d'une certaine flexibilité quant aux modalités d'établissement de leurs exigences pour ce secteur. En application d'autres dispositions figurant dans l'Annexe 6, Partie 2 — *Aviation générale internationale — Avions*, l'État d'immatriculation doit établir des critères pour les exploitants de l'AGI concernant la mise en œuvre d'un SGS.

8.4.7.5 L'établissement de ces critères devrait exiger l'application du cadre pour un SGS décrit à l'Annexe 19, mais cela peut se faire de diverses manières :

a) les critères sont établis dans le cadre des règlements d'exploitation spécifiques existants pour l'AGI ;

b) la publication des exigences dans le cadre réglementaire d'un instrument juridique autre que les règlements d'exploitation spécifiques qui définit les critères ;

c) le cadre réglementaire comporte des références à un code de pratiques de l'industrie pour les SGS qui est reconnu par l'État.

8.4.7.6 Lorsqu'il sélectionne la meilleure approche pour l'établissement des critères pour les SGS de l'AGI, l'État d'immatriculation devrait envisager comment le suivi du SGS sera effectué, y compris par une éventuelle délégation de la supervision à un tiers. Comme pour les SGS des prestataires de services, lorsqu'il s'agit de déterminer l'acceptabilité du SGS, l'État d'immatriculation devrait permettre une variabilité selon la taille, l'environnement d'exploitation et la complexité de l'exploitation.

8.4.7.7 Dans le cas d'un exploitant de l'AGI utilisant des aéronefs lourds ou à turboréacteurs immatriculés dans de multiples États et auquel un permis d'exploitation aérienne (AOC) a été délivré conformément à l'Annexe 6, Partie 1, ce dernier serait considéré comme un prestataire de services et traité comme tel, son SGS devant être rendu acceptable pour l'État de l'exploitant.

Acceptation du SGS

8.4.7.8 Beaucoup de prestataires de services ont des certificats, autorisations ou approbations de plus d'un État ou ont des activités dans plus d'un État. L'Annexe 19 ne contient aucune disposition imposant aux États de superviser le SGS d'un prestataire de services ne relevant pas de leur responsabilité. Toutefois, une harmonisation des exigences des SGS facilite l'acceptation des SGS entre États. L'harmonisation réduit les chevauchements d'activités de supervision et le besoin pour les prestataires de services de se conformer à des obligations de SGS similaires, imposées par des exigences (potentiellement) différentes. Les États devraient être attentifs aux politiques qui augmentent la charge administrative et financière des titulaires de certificats sans apporter de valeur ajoutée démontrable en matière de sécurité. Il importe de souligner que l'introduction du SGS a aggravé la situation pour les prestataires de services qui ne bénéficient pas de l'acceptation commune de leur certification, autorisation ou approbation. Les États devraient tenter de récolter les fruits de la mise en œuvre sans imposer une charge supplémentaire inutile aux prestataires de services.

8.4.7.9 De plus, les États sont encouragés à appliquer les exigences de la même manière lorsqu'ils octroient des certificats, autorisations ou approbations à des prestataires de services d'autres États, sans charges techniques, juridiques et administratives excessives. Nombre de prestataires de services ont besoin de ressources supplémentaires pour obtenir une acceptation initiale de plusieurs États et pour soutenir le suivi ou les audits périodiques d'États qui n'ont pas accepté leur SGS. Des efforts supplémentaires sont aussi requis lorsque les exigences varient, sont interprétées différemment ou sont conflictuelles.

8.4.7.10 L'Annexe 19 énonce les exigences-cadres pour le SGS. Les États transposent ces exigences dans leur cadre réglementaire. La performance de tout système ou processus organisationnel dépend, dans la pratique, des modalités d'application des exigences. Deux grands composants entrent en jeu dans l'équivalence des SGS et dans les implications de l'acceptation des SGS entre États.

8.4.7.11 Le premier concerne les aspects formels de la reconnaissance ou de l'acceptation du SGS. Certains États ont résolu cela par le biais d'accords bilatéraux ou multilatéraux recelant une combinaison d'arrangements diplomatiques, juridiques et techniques entre États. Dans certains cas, l'acceptation est mutuelle, mais pas dans toutes les circonstances.

8.4.7.12 Le deuxième composant est l'équivalence technique. L'équivalence technique peut être subdivisée en cinq aspects :

a) *Exigences communes*. Bien qu'insuffisante pour établir l'équivalence, l'utilisation d'un ensemble commun d'exigences assure structure et efficience aux évaluations techniques. Celles-ci ont été établies dans diverses Annexes de l'OACI.

b) *Attentes concernant la mise en œuvre*. Chaque État identifie des attentes spécifiques pour les processus, programmes, méthodes et outils permettant à l'autre autorité de faire la preuve de la mise en œuvre et de la performance.

c) *Méthodologie d'acceptation.* Les méthodes utilisées par les États pour évaluer comment les processus et capacités de gestion varient entre les États. Il s'agit généralement d'une fonction du système de supervision de la sécurité de l'État (EC-6, obligations en matière de délivrance de licences, de certifications, de permis, d'autorisation ou d'approbation).

d) *Mesure de la performance*. La méthodologie utilisée par chaque État pour mesurer la performance de sécurité des organisations qui ont été certifiées et approuvées vise à améliorer la compréhension qu'a l'État du potentiel de performance et de la situation de chaque organisation.

e) *Politiques et méthodes de suivi*. Le suivi doit garantir la performance des organisations et de leurs SGS. Il fait partie des obligations de surveillance de l'État. Chaque État doit acquérir une compréhension et une confiance dans les méthodes utilisées par une autre autorité pour superviser ses SGS. Cette compréhension et cette confiance soutiendront l'acceptation ou la reconnaissance des SGS.

8.4.7.13 Les SGS des prestataires de services doivent être rendus acceptables pour l'autorité nationale pertinente. Les prestataires de services sont tenus d'effectuer une analyse des lacunes et d'élaborer un plan de mise en œuvre réaliste (et prévoir son acceptation par l'État en tant que tâche planifiée). Les mises en œuvre des SGS sont généralement réalisées en trois ou quatre étapes. Une collaboration précoce entre le prestataire de services et les autorités de l'État facilitera probablement le processus d'élaboration et d'acceptation. Pour plus d'informations sur la mise en œuvre des SGS, voir le Chapitre 9.

Acceptation des SPI et des SPT

8.4.7.14 Les SPI proposés par les prestataires de services sont examinés et acceptés par l'autorité de réglementation compétente de l'État, dans le cadre du processus d'acceptation du SGS. Les États pourraient envisager de planifier l'acceptation des SPI des prestataires de services plus tard au cours du processus de mise en œuvre. Ce report est surtout pratique pour les prestataires de services lors d'une certification initiale car ils n'ont souvent pas assez de données pour élaborer des indicateurs utiles. L'autorité de réglementation peut avoir la certitude que les SPI proposés sont appropriés et correspondent bien aux activités d'aviation du prestataire de services concerné. Certains des SPI et SPT des prestataires de services peuvent être liés aux SPI et SPT de l'État pour la mesure et le suivi de l'ALoSP. Ce lien n'est pas nécessaire pour tous les SPI et SPT. De plus amples informations sur la mesure de la performance de sécurité figurent au Chapitre 4.

8.4.7.15 L'acceptation des SPT du prestataire de services peut être traitée après que les SPI ont été suivis pendant un certain temps. Cela permet d'établir la performance de référence. Celle-ci peut être basée sur les cibles établies au niveau national, régional ou mondial. La réalisation des SPT de l'État exigera la coordination des actions d'atténuation des risques de sécurité avec le prestataire de services.

Un SGS pour de multiples prestataires de services

8.4.7.16 Des organisations titulaires de multiples certifications de prestataires de services peuvent choisir de les inclure toutes dans le champ d'application d'un seul SGS pour tirer parti des avantages du SGS et mieux gérer les aspects liés aux interfaces. L'autorité de réglementation de l'État devrait envisager les points suivants lorsqu'elle évalue le SGS de ces organisations apparentées ou la mise en œuvre des exigences du SGS pour les prestataires de services inclus dans le champ d'application d'un SGS plus large :

a) Veiller à ce que les politiques et processus de suivi du SGS soient appliqués de façon cohérente dans l'ensemble de l'État, en particulier lorsque des inspecteurs d'organisations différentes au sein de l'autorité de réglementation sont chargés de la supervision et du suivi des différents prestataires de services :

1) il existe des preuves d'engagement de la direction en faveur d'une interprétation cohérente des réglementations et de l'application de la supervision et du suivi ;

2) tout le personnel chargé de la supervision et du suivi a reçu une formation normalisée ; idéalement, ce personnel doit compter des participants de différentes disciplines ;

3) des politiques, procédures et outils d'audit communs doivent être élaborés et mis en œuvre lorsque différentes organisations assurent la supervision et le suivi ;

4) il y a une communication cohérente et fréquente entre les inspecteurs responsables affectés à chaque prestataire de services ;

5) des mécanismes sont en place pour surveiller le degré de normalisation des activités de supervision et de suivi. Tout problème identifié doit être traité ;

6) il est reconnu que les activités du prestataire de services peuvent être traitées par le SGS au niveau de l'entreprise (« société mère »). Cela peut inclure des activités qui exigent un SGS et des activités ne relevant pas du champ d'application de l'Annexe 19 ;

7) l'organisation mère a documenté :

i) ses politiques et procédures en précisant comment les données de sécurité et les informations de sécurité sont partagées, les communications sont relayées, les décisions sont prises et les ressources sont affectées aux différents domaines d'activités et, le cas échéant, avec différentes autorités de réglementation ;

ii) les rôles et responsabilités associés à son SGS et le cadre d'obligations de rendre compte pour le SGS ;

iii) la structure organisationnelle et les interfaces entre différents systèmes et activités dans la description de son système.

b) Veiller à sensibiliser au fait que des organisations mères détenant de multiples certificats — dont certains délivrés par des autorités de réglementation étrangères — peuvent choisir de mettre en œuvre un seul SGS pour les multiples prestataires de services :

1) reconnaître que la portée d'un SGS est clairement définie dans la description du système et que les différentes activités sont exposées en détail. Le prestataire de services peut prouver la compatibilité entre ses processus de SGS et le SGS de l'entreprise ;

2) être conscient que ce scénario peut générer des défis supplémentaires lorsque l'organisation mère est titulaire d'approbations tant nationales qu'internationales, telles que l'acceptation du SGS par différentes autorités de réglementation. Un accord devrait être passé avec les autres autorités de réglementation sur la façon dont la supervision et le suivi seront partagés, délégués ou maintenus séparés (dupliqués) lorsque des arrangements pour l'acceptation du SGS n'ont pas encore été établis.

Systèmes de gestion intégrés

8.4.7.17 L'autorité de réglementation devrait envisager les points suivants lorsqu'elle évalue les prestataires de services qui ont intégré leur SGS avec d'autres systèmes de gestion :

a) rédiger une politique qui clarifie la portée de ses compétences (elle n'est peut-être pas responsable de la supervision des systèmes de gestion connexes) ;

b) les ressources nécessaires pour évaluer et assurer le suivi d'un système de gestion intégré (elles pourraient inclure du personnel ayant les savoir-faire appropriés, des processus, des procédures et des outils).

8.4.7.18 Il y a des avantages pour le prestataire de services à intégrer son SGS avec d'autres systèmes de gestion. L'intégration devrait être terminée à la satisfaction de l'AAC et de telle manière que l'AAC puisse effectivement « voir » le SGS et en assurer le suivi. Des orientations destinées aux prestataires de services qui mettent en œuvre un SGS en tant que partie d'un système de gestion intégré sont disponibles au Chapitre 9.

8.4.8 Enquêtes sur les accidents

8.4.8.1 Le service d'enquête sur les accidents (AIA) doit être fonctionnellement indépendant de toute autre organisation. Il est particulièrement important qu'il soit indépendant de l'AAC de l'État. Les intérêts de l'AAC pourraient entrer en conflit avec les tâches confiées à l'AIA. L'indépendance de cette fonction par rapport à d'autres organisations est nécessaire parce que les causes d'accidents peuvent être liées à des facteurs réglementaires ou à des facteurs liés au PNS. De plus, une telle indépendance renforce la viabilité de l'AIA et prévient des conflits d'intérêts réels ou perçus.

8.4.8.2 Le processus d'enquête sur les accidents a un rôle central à jouer dans le PNS. Il permet à l'État d'identifier des facteurs contributifs et toute défaillance possible au sein du système aéronautique et de générer les contre-mesures nécessaires pour prévenir une récurrence. Cette activité contribue à l'amélioration continue de la sécurité de l'aviation en mettant au jour des défaillances actives et des facteurs contributifs d'accidents/incidents et en fournissant des rapports sur les leçons tirées de l'analyse d'événements. Ce travail peut soutenir l'adoption de mesures correctrices et l'affectation correspondante de ressources et peut identifier les améliorations nécessaires à apporter au système aéronautique. Pour plus d'informations, voir l'Annexe 13 de l'OACI et les orientations connexes.

8.4.8.3 Beaucoup d'événements de sécurité ne requièrent pas une enquête officielle en application de l'Annexe 13. Ces événements et les dangers identifiés peuvent être des indices de problèmes systémiques. Ces problèmes peuvent être révélés et résolus par une enquête en matière de sécurité menée par le prestataire de services. Pour plus d'informations sur les enquêtes en matière de sécurité menées par le prestataire de services, voir le Chapitre 9.

8.4.9 Identification des dangers et évaluation des risques de sécurité

Éléments indicatifs généraux

8.4.9.1 Un des rôles les plus importants des autorités aéronautiques est d'identifier les dangers et les tendances émergentes dans l'ensemble du système aéronautique. Ce travail est souvent réalisé en analysant les données de sécurité agrégées provenant de multiples sources. Le niveau de complexité et de sophistication du processus de GRS des États varie en fonction de la taille, de la maturité et de la complexité du système aéronautique de chaque État. Des éléments indicatifs généraux sur le processus de GRS figurent au Chapitre 2.

8.4.9.2 La collecte de données de sécurité et d'informations de sécurité tant internes qu'externes est essentielle pour parvenir à créer un PNS efficace. Des systèmes aéronautiques non complexes peuvent produire peu de données. Dans ce cas, la collecte et l'échange de données externes devraient être une priorité. Des données externes sont souvent disponibles auprès d'autres États ; il s'agit entre autres de rapports d'enquêtes, de rapports de sécurité annuels (comprenant des informations et analyses relatives à des incidents), d'alertes de sécurité, de bulletins de sécurité, d'études sur la sécurité, d'iSTARS, etc. Au niveau régional, les groupes de l'OACI (p. ex. RASG, groupes régionaux de planification et de mise en œuvre [PIRG], etc.) peuvent aussi constituer de bonnes sources d'informations de sécurité. Le système de collecte et de traitement des données de sécurité (SDCPS) de l'État devrait comporter des procédures pour le dépôt à l'OACI de rapports sur les accidents et les incidents, ce qui faciliterait la collecte et le partage d'informations de sécurité mondiales.

8.4.9.3 Le but premier de la GRS est d'identifier et de maîtriser les conséquences potentielles de dangers en utilisant les données de sécurité disponibles. Les principes de la GRS sont les mêmes pour les États et les prestataires de services.

8.4.9.4 Les prestataires de services ont accès à leurs propres données de sécurité. Les États ont accès aux données de sécurité de multiples prestataires de services. Par conséquent, en mettant en œuvre des taxonomies communes pour classer les données de sécurité qu'il collecte, l'État améliorera grandement l'efficacité de son processus de GRS. Cela permet aussi de réaliser une analyse plus efficiente des données collectées auprès de multiples sources dans différents secteurs de l'aviation. Les intrants et extrants du processus d'analyse des données sont illustrés à la Figure 8-2 ci-dessous.

8.4.9.5 Des intrants peuvent être obtenus de n'importe quelle partie du système aéronautique. Il peut s'agir d'enquêtes sur des accidents, d'enquêtes en matière de sécurité réalisées par un prestataire de services, de rapports de maintien de la navigabilité, de résultats d'évaluations médicales, d'évaluations des risques de sécurité, de constatations d'audits et de rapports d'audits, d'études et d'analyses de la sécurité.

8.4.9.6 Si nécessaire, des extrants ou des mesures de maîtrise des risques de sécurité sont appliqués pour éliminer le danger ou pour réduire le risque de sécurité à un niveau acceptable. Voici quelques exemples des nombreuses options d'atténuation à la disposition des États : consignes de navigabilité, apport d'intrants pour affiner la supervision et le suivi du ou des prestataires de services, amendements à la certification, établissement de règles ou de politiques de sécurité, programme de promotion de la sécurité, facilitation des leçons tirées d'ateliers. L'action choisie dépendra manifestement de la gravité et du type de problème traité.

Identification des dangers

8.4.9.7 L'identification des dangers repose sur la collecte de données représentatives. Il peut être approprié de combiner ou d'agréger des données de multiples secteurs pour garantir une compréhension complète de chaque danger. Le processus illustré à la Figure 8-2 est valable pour l'identification tant réactive que proactive des dangers. L'analyse des dangers identifiés pendant une enquête sur un incident ou un accident est un exemple de méthodologie réactive. Une méthodologie proactive pourrait inclure des dangers identifiés pendant des audits ou des inspections ou à partir de comptes rendus obligatoires. En cas de signes précoces de dégradation de la performance de sécurité, elle pourrait prévoir une alerte donnée par le suivi quotidien de la fiabilité du système.

8.4.9.8 Des dangers existent à tous les niveaux au sein du système aéronautique des États. Des accidents ou des incidents se produisent lorsque des dangers interagissent avec certains facteurs déclencheurs. En conséquence, les dangers devraient être identifiés avant qu'ils ne causent des accidents, des incidents ou d'autres événements liés à la sécurité.

8.4.9.9 Les États sont encouragés à désigner un individu ou une équipe chargés de collecter, agréger et analyser les données disponibles. Les analystes de la sécurité de l'État devraient analyser les données pour identifier et documenter les dangers potentiels ainsi que les effets ou les conséquences connexes. Le niveau de précision requis pour le processus d'identification des dangers dépend de la complexité du processus étudié.

8.4.9.10 Il faudrait établir un processus systématique pour garantir une identification efficace des dangers. Ce processus devrait comporter les éléments suivants :

a) un accès aux sources de données nécessaires pour soutenir la gestion des risques de sécurité au sein de l'État ;

b) une équipe d'analyse de la sécurité ayant les compétences analytiques et l'expérience opérationnelle appropriées, ainsi qu'une formation à et une expérience de tout un éventail de techniques d'analyse des dangers ;

c) un ou plusieurs outils d'analyse des dangers appropriés aux données en cours de collecte (ou à collecter) et à l'étendue des activités d'aviation de l'État.

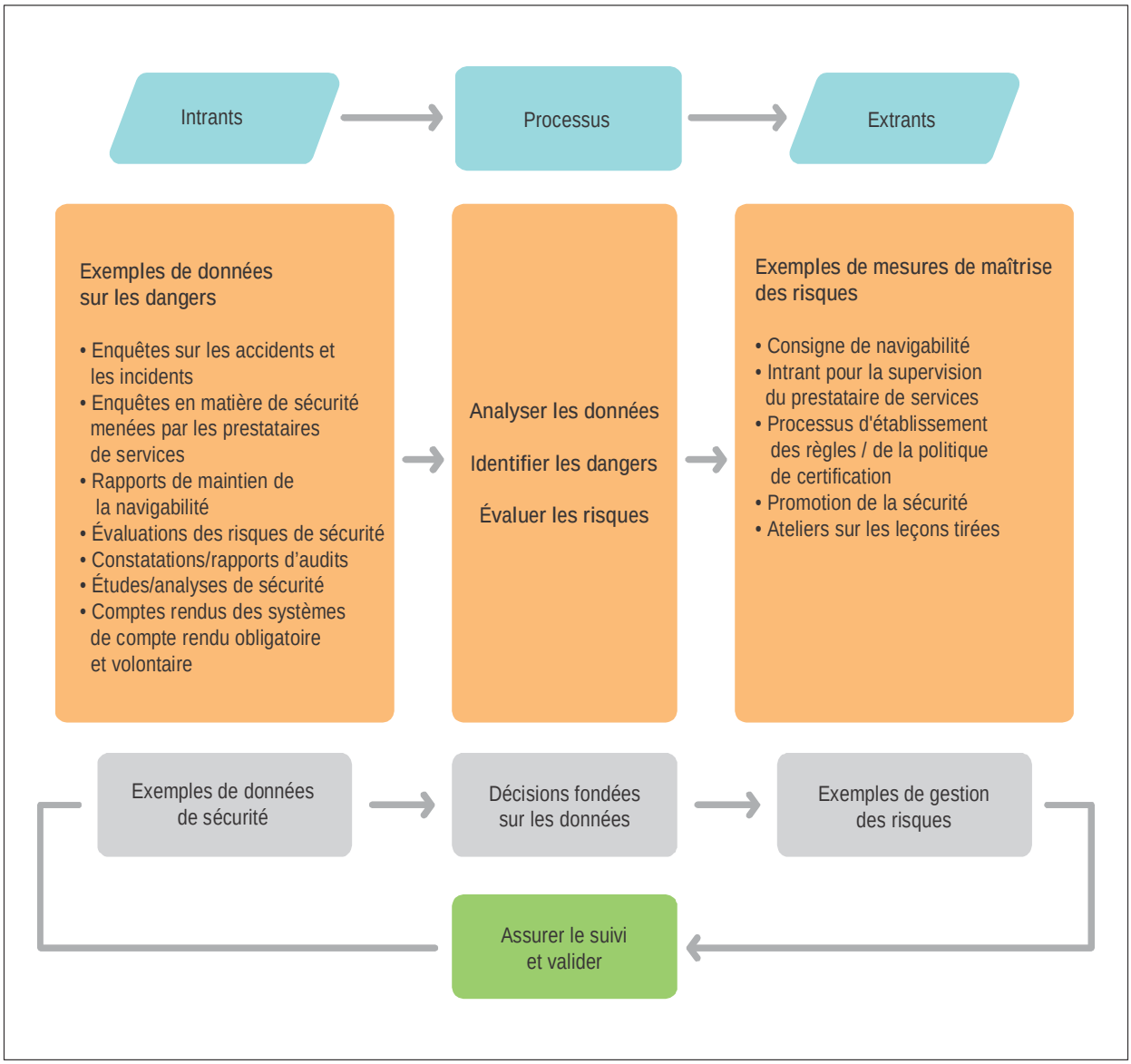

Figure 8-2. Programme d'analyse fondé sur les données

Facteurs déclencheurs d'identification de dangers

8.4.9.11 Il existe de nombreuses situations dans lesquelles il faudrait lancer une identification des dangers. Voici quelques exemples des principales :

a) *Conception du système :* L'identification des dangers commence avant le début des opérations par une description détaillée du système aéronautique concerné et de son environnement. L'équipe d'analyse de la sécurité identifie les divers dangers potentiels associés au système ainsi que les incidences de ces dangers sur d'autres systèmes en interface.

b) *Changement de système :* L'identification des dangers commence avant l'introduction d'un changement dans le système (opérationnel ou organisationnel) et inclut une description détaillée du changement

particulier à apporter au système aéronautique. L'équipe d'analyse de la sécurité identifie les dangers potentiels associés au changement proposé ainsi que les incidences de ces dangers sur d'autres systèmes en interface.

c) *Suivi à la demande et en continu :* L'identification des dangers est appliquée aux systèmes existants en fonctionnement. Le suivi des données est utilisé pour détecter des changements dans le bilan des dangers. Par exemple, les dangers peuvent se manifester de façon plus fréquente ou plus grave que prévu ou les stratégies d'atténuation convenues sont moins efficaces que prévu. Un suivi et une analyse continus peuvent être mis en place, avec notification de seuils, sur la base d'un ensemble d'éléments cruciaux dignes d'intérêt.

Évaluation des risques de sécurité

8.4.9.12 Des éléments indicatifs généraux sur l'évaluation des risques de sécurité figurent au Chapitre 2. Il convient de noter que les risques de sécurité peuvent être décelés et maîtrisés dans un secteur de l'aviation ou dans une région.

8.4.9.13 Il existe de nombreux outils pour analyser les données et utiliser différentes approches de modélisation des risques de sécurité. Lorsqu'ils sélectionnent ou élaborent des évaluations des risques de sécurité, les États devraient s'assurer que le processus fonctionne bien pour leur environnement.

8.4.10 Gestion des risques de sécurité

8.4.10.1 Des éléments indicatifs sur la résolution des problèmes de sécurité (EC-8) figurent dans le Doc 9734, Partie A.

8.4.10.2 La gestion des risques de sécurité a pour objectif de garantir que les risques de sécurité sont maîtrisés et qu'un ALoSP est atteint. L'autorité compétente de l'aviation de l'État élabore, documente et recommande des stratégies appropriées d'atténuation des risques de sécurité ou de maîtrise des risques de sécurité. En voici quelques exemples : intervention directe auprès d'un prestataire de services, mise en œuvre de politiques ou de réglementations supplémentaires, publication de consignes d'exploitation ou influence au moyen d'activités de promotion de la sécurité.

8.4.10.3 Chaque mesure proposée de maîtrise des risques de sécurité devrait ensuite faire l'objet d'une évaluation. Les mesures de maîtrise des risques de sécurité possibles et idéales sont rentables, faciles à exécuter, rapidement mises en œuvre, efficaces et ne génèrent pas de conséquences involontaires. Comme la plupart des situations ne répondent pas à ces critères idéaux, les mesures de maîtrise des risques de sécurité possibles devraient être évaluées et sélectionnées en fonction d'une recherche d'un équilibre entre les caractéristiques d'efficacité, de coût, d'opportunité de mise en œuvre et de complexité. Une fois sélectionnées et mises en œuvre, les mesures de maîtrise des risques de sécurité devraient faire l'objet d'un suivi et être validées afin de garantir que les buts escomptés ont été atteints.

8.4.10.4 Nombre de mesures de maîtrise des risques de sécurité requièrent une action de la part du ou des prestataires de services. Les États devraient ordonner aux prestataires de services de procéder à une mise en œuvre efficace. Les États devront peut-être assurer le suivi de l'efficacité des mesures de maîtrise des risques de sécurité et de leur incidence sur la performance de sécurité des prestataires de services et, collectivement, des États. Les approches de l'atténuation des risques de sécurité sont exposées au Chapitre 2.

8.5 COMPOSANT 3 : ASSURANCE DE LA SÉCURITÉ PAR L'ÉTAT

8.5.1 Les activités d'assurance de la sécurité menées par l'État visent à garantir à l'État que ses fonctions atteignent leurs objectifs et cibles de sécurité prévus. Les prestataires de services sont tenus de mettre en œuvre un

processus d'assurance de la sécurité dans le cadre de leur SGS. La capacité d'assurance de la sécurité du SGS garantit à chaque prestataire de services que ses processus de sécurité fonctionnent correctement et qu'il est en bonne voie pour atteindre ses objectifs de sécurité. De même, les activités d'assurance de la sécurité de l'État, menées dans le cadre du PNS, donnent à l'État l'assurance que ses processus de sécurité fonctionnent correctement et que l'État est en voie d'atteindre ses objectifs de sécurité par le biais des efforts collectifs du secteur aéronautique de l'État.

8.5.2 Les activités de surveillance et les mécanismes de collecte, analyse, partage et échange de données/informations de sécurité garantissent que les mesures réglementaires de maîtrise des risques de sécurité sont intégrées de façon appropriée dans le SGS du prestataire de services. Cela donne l'assurance que le système est appliqué tel qu'il a été conçu et que les contrôles réglementaires ont l'effet escompté sur la GRS. Les États peuvent collecter des données/informations de sécurité sur l'aviation auprès de nombreuses sources, y compris par des processus de surveillance et des programmes de compte rendu de sécurité. Les données devraient être analysées à divers niveaux et les conclusions tirées de l'analyse devraient être utilisées comme base pour prendre des décisions de sécurité en connaissance de cause concernant les activités de surveillance et la sécurité du système aéronautique de l'État.

8.5.3 Obligations de surveillance

8.5.3.1 Des éléments indicatifs sur les obligations de surveillance (EC-7) relatives au suivi de la conformité figurent dans le Doc 9734, Partie A.

Priorisation des activités de surveillance

8.5.3.2 Une approche de la surveillance fondée sur le risque pour la sécurité (SRBS) permet de prioriser et de répartir les ressources de gestion de la sécurité de l'État proportionnellement au profil de risque de sécurité de chaque secteur ou de chaque prestataire de services. Les États améliorent leur expérience et leur connaissance de chaque prestataire de services en surveillant la progression constante de la maturité de leur processus d'assurance de la sécurité et, en particulier, leur gestion de la performance de sécurité. Au fil du temps, l'État acquerra une image claire des capacités du prestataire de services en matière de sécurité, en particulier de sa gestion des risques de sécurité. L'État peut choisir de modifier la portée et/ou la fréquence de sa surveillance à mesure que se renforce sa confiance dans les capacités de sécurité du prestataire de services et qu'il en récolte des preuves.

8.5.3.3 La SRBS est surtout appropriée pour des organisations ayant un SGS arrivé à maturité. Elle peut aussi s'appliquer à des organisations dont le SGS n'a pas encore été mis en œuvre. Une SRBS efficace repose sur des données qui sont suffisamment fiables et utiles. En l'absence de données fiables et utiles, il est difficile de défendre des ajustements de la portée ou de la fréquence de la surveillance.

8.5.3.4 Les États devraient développer ou renforcer leurs capacités de gestion des données afin de s'assurer qu'ils disposent de données fiables et complètes sur lesquelles baser leurs décisions (fondées sur les données). Les analyses des risques de sécurité par secteur peuvent aussi permettre à l'État d'évaluer les risques de sécurité communs qui affectent de multiples prestataires de services pratiquant des types d'activités similaires (p. ex. compagnies aériennes effectuant des vols court-courriers). Cela facilite le classement des risques de sécurité parmi les prestataires de services au sein d'un secteur spécifique de l'aviation ou sur une base transsectorielle et soutient l'affectation des ressources de surveillance à des secteurs ou activités où l'effet sur la sécurité sera le plus grand.

8.5.3.5 Les analyses au niveau des secteurs permettent à l'État de visualiser le système aéronautique dans son contexte, c'est-à-dire de voir comment les parties contribuent au tout. Elles donnent à l'État la capacité d'identifier quels secteurs bénéficieront de niveaux accrus d'appui ou d'intervention et quels secteurs sont les plus adaptés pour une approche plus collaborative. L'État acquiert ainsi l'assurance que la réglementation pour l'ensemble du système aéronautique est proportionnée et qu'elle cible les domaines où les besoins sont les plus criants. Il est plus aisé d'identifier où des changements de réglementations spécifiques sont requis pour atteindre l'efficacité maximale de la réglementation avec le moins d'ingérence possible.

8.5.3.6 La SRBS a un coût. Elle exige des interactions constantes entre l'État et la communauté aéronautique au-delà des audits et inspections fondés sur la conformité. Une approche de la SRBS utilise le profil de risque de sécurité du prestataire de services pour adapter ses activités de surveillance. Les extrants des examens, analyses et prises de décisions internes au sein du système du prestataire de services deviennent un plan d'action ciblé qui traite les risques de sécurité principaux et les mesures d'atténuation qui les résoudront efficacement. L'analyse à la fois de l'État et du prestataire de services définit les domaines prioritaires en matière de préoccupations de sécurité et détermine les moyens les plus efficaces pour y remédier.

8.5.3.7 Point important, la surveillance fondée sur les risques de sécurité ne réduira pas nécessairement le volume de surveillance effectué ou les ressources requises ; par contre, la qualité de la surveillance et la qualité de l'interaction entre l'autorité de réglementation et le prestataire de services s'en trouveront grandement améliorées.

Profils de risques de sécurité organisationnels du prestataire de services

8.5.3.8 Les États pourraient souhaiter élaborer des profils de risques de sécurité organisationnels cohérents pour chaque secteur de l'aviation, afin d'appuyer le processus de modification de la portée et de la fréquence de leurs activités de surveillance. Ces outils devraient viser à saisir et à agréger les informations qui devraient être déjà disponibles pour les prestataires de services et pourraient inclure des facteurs tels que :

a) la santé financière de l'organisation ;

b) le nombre d'années d'exploitation ;

c) le taux de rotation du personnel clé, notamment du dirigeant responsable et du gestionnaire de la sécurité ;

d) la compétence et la performance du dirigeant responsable ;

e) la compétence et la performance du gestionnaire de la sécurité (pour plus d'informations sur la compétence du dirigeant responsable et du gestionnaire de la sécurité, voir le Chapitre 9) ;

f) les résultats d'audits précédents ;

g) la résolution efficace et en temps utile des constatations précédentes ;

h) les mesures du niveau relatif d'activité (exposition au risque de sécurité) ;

i) les indicateurs de la portée et de la complexité relatives des activités effectuées ;

j) la maturité du processus d'identification des dangers et d'évaluation des risques de sécurité ;

k) les mesures de la performance de sécurité à partir des activités d'analyse des données de sécurité et de suivi de la performance menées par l'État.

8.5.3.9 La Figure 8-3 présente un exemple d'un processus qui peut être utilisé pour modifier la portée ou la fréquence de la surveillance d'un prestataire de services.

8.5.4 Suivi de la performance de sécurité d'un prestataire de services

L'État devrait réexaminer périodiquement les SPI et les SPT de chaque prestataire de services. Cet examen devrait prendre en considération la performance et l'efficacité de chaque SPI et SPT. Il peut révéler la nécessité d'apporter des ajustements pour soutenir l'amélioration continue de la sécurité.

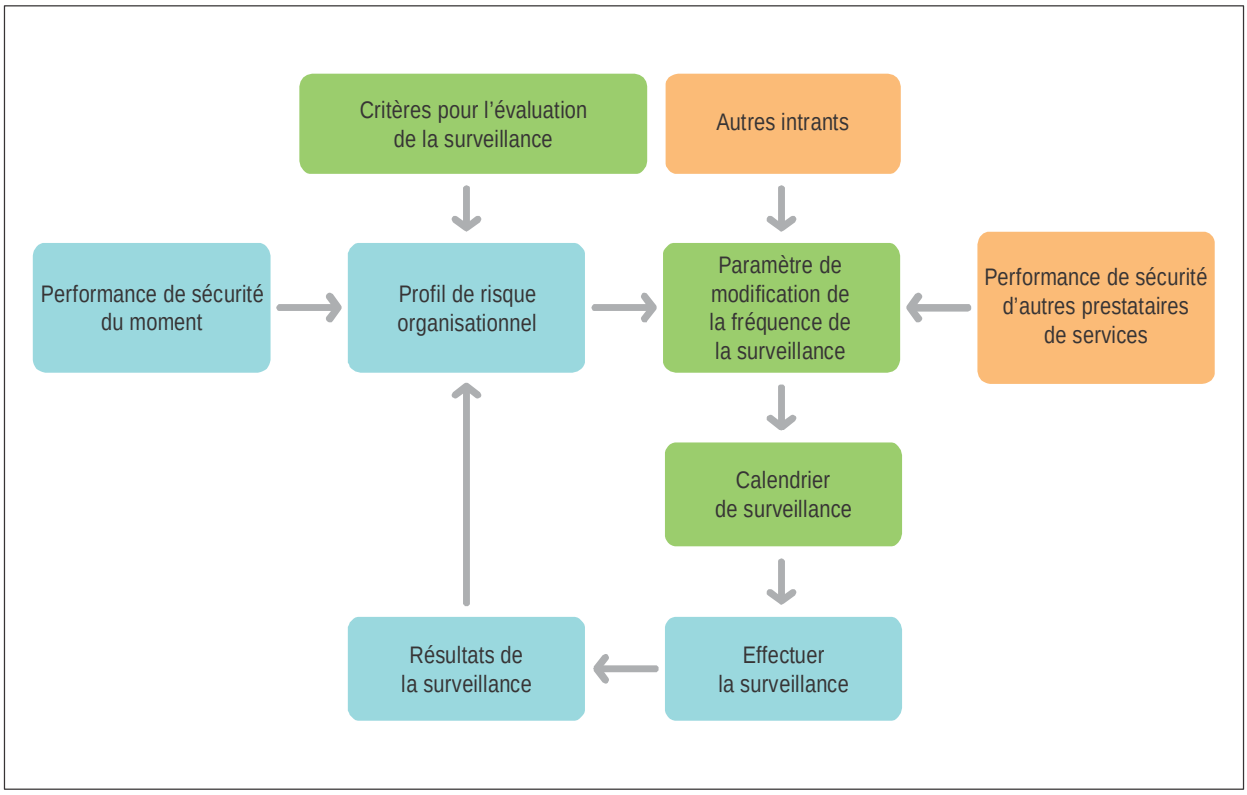

Figure 8-3. Concept de surveillance fondée sur le risque de sécurité

8.5.5 Performance de sécurité de l'État

8.5.5.1 Des informations générales sur la gestion de la performance de sécurité sont données au Chapitre 4.

Niveau acceptable de performance de sécurité

8.5.5.2 Les États sont tenus d'établir le niveau acceptable de performance de sécurité (ALoSP) à atteindre dans le cadre de leur PNS. Pour ce faire, ils peuvent :

a) mettre en œuvre et tenir à jour le PNS ;

b) mettre en œuvre et tenir à jour les SPI et les SPT en montrant que la sécurité est gérée avec efficacité.

8.5.5.3 L'ALoSP exprime les niveaux de sécurité que l'État attend de son système aéronautique, y compris les cibles que chaque secteur doit atteindre et maintenir en matière de sécurité, ainsi que les mesures visant à déterminer l'efficacité de ses propres activités et fonctions qui ont une incidence sur la sécurité. L'ALoSP reflète donc les aspects que l'État considère comme importants et qui sont convenus par les parties prenantes de l'aviation à l'échelon de l'État. L'ALoSP ne devrait pas être établi isolément. Au contraire, il faudrait le définir en tenant compte d'orientations stratégiques de niveau supérieur (du GASP, des plans régionaux, etc.) et des objectifs de sécurité établis dans le PNS.

Établissement de l'ALoSP

8.5.5.4 La responsabilité de l'établissement de l'ALoSP incombe aux autorités aéronautiques de l'État et sera exprimée par le biais de l'ensemble des SPI établis pour l'État, les secteurs et les prestataires de services relevant de la compétence de ces autorités. Le but est de maintenir ou de constamment améliorer la performance de sécurité du processus de mesure de l'ensemble du système aéronautique décrit au Chapitre 4. Cela permet à l'État de comprendre où il en est sur le plan de la sécurité et d'agir pour influer sur la situation, si nécessaire. L'acceptation des SPI et des cibles des prestataires de services fait partie de ce processus.

8.5.5.5 L'ALoSP représente l'accord passé entre toutes les autorités en charge de l'aviation au sein d'un État, sur le niveau attendu de performance de sécurité que le système aéronautique de cet État devrait atteindre et il montre aux parties prenantes internes et externes comment l'État gère la sécurité de l'aviation. Il inclut, mais sans s'y limiter, la performance de sécurité de chaque secteur et de chaque prestataire de services relevant de la juridiction de l'État. L'établissement d'un ALoSP ne remplace ni ne supplante l'obligation d'un État de respecter la Convention relative à l'aviation civile internationale et, notamment, de mettre en œuvre toutes les SARP applicables.

8.5.5.6 La Figure 8-4 décrit le concept de l'ALoSP sur la base des SPI et des SPT. De plus amples indications sur les objectifs de sécurité, les SPI et les SPT figurent au Chapitre 4 et dans les paragraphes suivants.

Indicateurs de performance de sécurité et cibles de performance de sécurité

8.5.5.7 Des SPI utiles devraient refléter l'environnement d'exploitation spécifique et servir à mettre en lumière les circonstances qui peuvent être utilisées pour identifier comment les risques de sécurité sont maîtrisés. La stratégie de suivi et de mesure appliquée par l'État devrait inclure un ensemble de SPI qui couvre tous les domaines du système aéronautique dont l'État est responsable. Elle devrait refléter à la fois les résultats (p. ex. accidents, incidents, violations des réglementations) et les fonctions et activités (opérations pour lesquelles les mesures d'atténuation des risques en place ont fonctionné comme prévu). Cette combinaison permet d'évaluer la performance de sécurité sur la base non seulement de ce qui ne fonctionne pas (à savoir les résultats) mais aussi de ce qui fonctionne (à savoir les activités pour lesquelles les mesures d'atténuation des risques de sécurité ont produit les effets escomptés). Dans la pratique, cette approche prend en compte les SPI qui reflètent deux types distincts de risques de sécurité :

a) **Les risques liés à la sécurité opérationnelle** (illustrés du côté gauche du diagramme) se concentrent sur les circonstances qui pourraient mener à un résultat non souhaité. Il s'agit de circonstances associées à des accidents, incidents, défaillances et défauts. Le risque lié à la sécurité opérationnelle est essentiellement un sous-produit de la prestation de services. C'est pourquoi les SPI centrés sur le risque lié à la sécurité opérationnelle seront surtout liés — indirectement — aux SGS des prestataires de services. Bien que la Figure 8-4 illustre trois risques liés à la sécurité opérationnelle, le nombre réel devrait être basé sur la situation dans chaque État.

   Ces SPI reflètent principalement les problèmes de sécurité opérationnelle identifiés par le processus de GRS des prestataires de services. Le processus de GRS de l'État peut aussi être utilisé comme intrant reflétant les problèmes de sécurité opérationnelle décelés dans l'ensemble du système aéronautique de l'État à partir de l'agrégation des SPI des prestataires de services relatifs aux risques liés à la sécurité opérationnelle. Un problème de sécurité opérationnelle est souvent corrélé à plusieurs SPI connexes. En d'autres termes, un problème de sécurité opérationnelle peut être révélé par plusieurs SPI.

b) **Les risques de sécurité liés à la mise en œuvre des processus** (illustrés du côté droit du diagramme) se concentrent sur les moyens et ressources nécessaires pour gérer le risque de sécurité opérationnelle. La gestion des risques de sécurité envisagée sous l'angle de la mise en œuvre des processus commence par l'évaluation du degré de mise en œuvre des SARP de l'OACI (lois et réglementations nationales liées à la sécurité), de la mise en œuvre des processus des SGS dans l'industrie, et de la mise en œuvre du PNS au niveau de l'État (qui inclut une supervision et un suivi efficaces de l'industrie).

Si des améliorations à l'un quelconque des éléments susmentionnés sont nécessaires, les activités pour atteindre les niveaux requis devraient être planifiées, mises en œuvre et suivies et des ressources adéquates devraient être affectées à ces activités. Des SPI sont ensuite élaborés pour permettre un suivi de la planification, de la mise en œuvre et/ou de l'efficacité des changements.

Les SPI concentrés sur le « risque de sécurité lié à la mise en œuvre des processus » fournissent à l'État un autre moyen que la stricte conformité pour surveiller l'adéquation des arrangements institutionnels liés aux SGS et la mise en œuvre des processus de GRS/assurance de la sécurité par les prestataires de services. Ces SPI peuvent aussi être établis en référence à des améliorations nécessaires, comme indiqué par les analyses de l'USOAP et les activités d'amélioration continue du PNS. Les résultats des audits USOAP, de l'agrégation des évaluations des SGS et des informations sur l'amélioration continue du PNS déterminent les domaines potentiels d'amélioration. Ceux-ci devraient être priorisés selon leur degré d'intérêt. Cela contribuera à améliorer la performance de sécurité du système aéronautique de l'État. Ces SPI devraient être distincts des SPI concernant les risques liés à la sécurité opérationnelle.

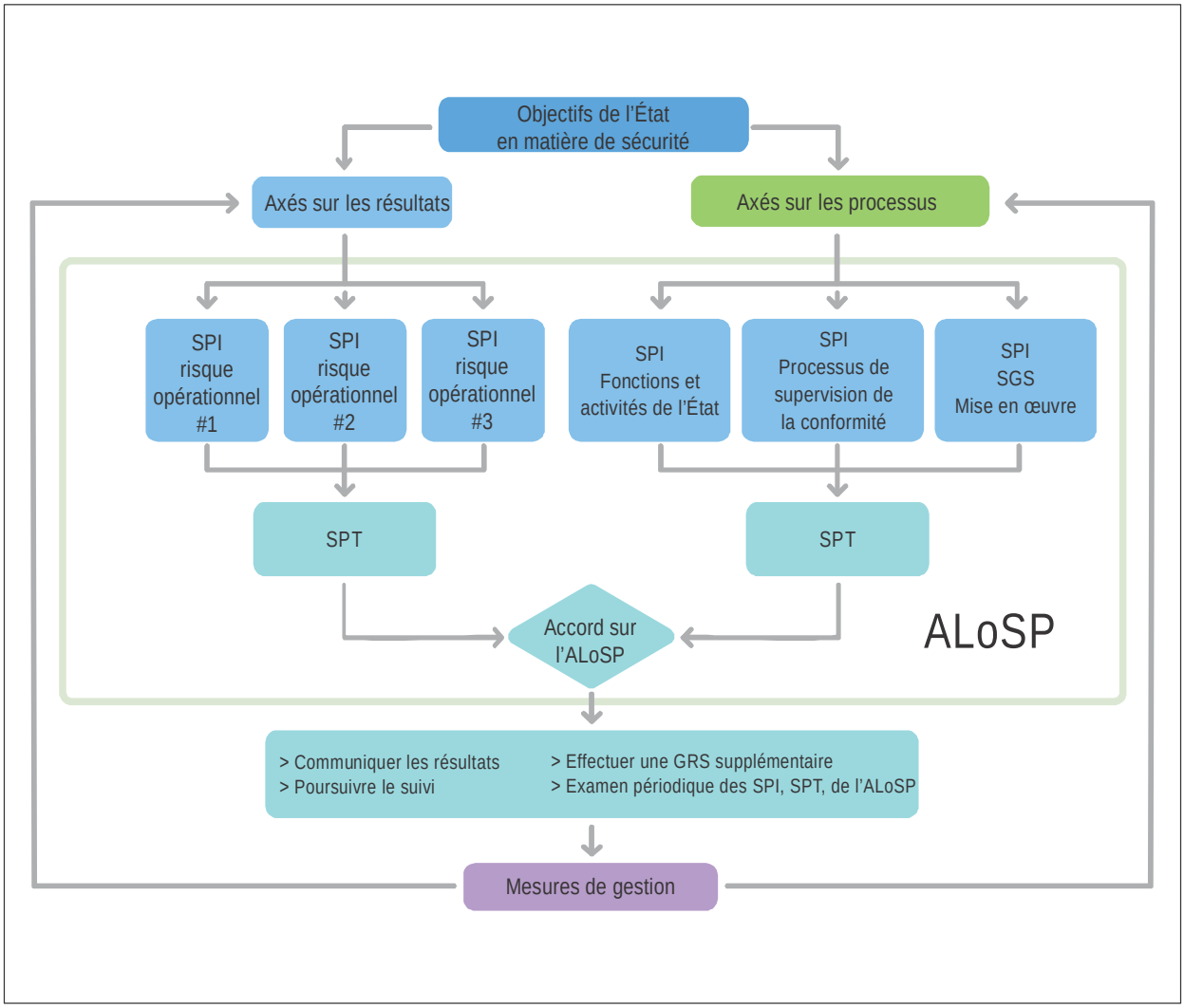

Figure 8-4. Niveau acceptable de performance de sécurité (ALoSP)

8.5.5.8 Les SPI établis tant pour les risques liés à la sécurité opérationnelle que pour les risques liés à la mise en œuvre des processus constituent une partie fondamentale du processus d'assurance de la sécurité de l'État. L'agrégation des SPI pour les risques liés à la sécurité opérationnelle et des SPI pour les risques liés à la mise en œuvre des processus élargit la source de rétro-informations permettant d'établir l'ALoSP de l'État.

Examen périodique des indicateurs de performance de sécurité

8.5.5.9 Un examen périodique est essentiel une fois que les SPI de l'État sont établis. Initialement, l'identification des principaux risques de sécurité est une activité soutenue par l'analyse basée sur des données historiques. Toutefois, le système aéronautique est dynamique et en constante évolution. De nouveaux problèmes de sécurité peuvent se poser, les processus au sein d'un État peuvent changer, etc. Un examen périodique des problèmes et processus de l'État relatifs à la sécurité opérationnelle soutient l'actualisation et l'affinement des objectifs de sécurité de l'État et, en conséquence, des SPI et des SPT.

Examen périodique de l'ALoSP

8.5.5.10 L'équipe de la haute direction qui est responsable de l'accord d'origine sur l'ALoSP devrait déterminer si l'ALoSP reste approprié. L'examen périodique de l'ALoSP devrait viser à :

a) identifier les problèmes de sécurité critiques au sein des secteurs de l'aviation, en assurant l'inclusion de SPI qui permettent une gestion de la performance de sécurité dans ces domaines ;

b) identifier des SPT qui définissent le niveau de performance de sécurité à maintenir ou l'amélioration souhaitée à atteindre pour le SPI pertinent de chaque secteur, en vue de renforcer la gestion de la performance de sécurité dans l'ensemble du système aéronautique de l'État ;

c) identifier les facteurs déclencheurs (le cas échéant) lorsqu'un SPI atteint un point qui requiert la prise de mesures ;

d) revoir les SPI pour déterminer si des modifications ou des ajouts aux SPI, SPT et facteurs déclencheurs (le cas échéant) existants sont nécessaires pour atteindre l'ALoSP convenu.

8.5.5.11 L'examen périodique des principaux risques de l'État offre une meilleure compréhension de la nature de chaque problème de sécurité opérationnelle avec le degré de précision maximal que permettent les données. L'État devrait prendre en considération ses dangers et leurs conséquences potentielles à tous les niveaux du système aéronautique de l'État. Il devrait aussi analyser comment les processus de l'État (délivrance de licences, certification, autorisation, approbation, activités de surveillance, etc.) contribuent à la GRS. Chaque risque lié à la sécurité opérationnelle est évalué pour identifier les mesures d'atténuation des risques de sécurité requises. Le suivi de ces actions est assuré par le biais de SPI qui mesurent leur efficacité.

8.5.5.12 L'amélioration de la performance de sécurité relative aux risques liés à la sécurité opérationnelle tend à être un processus réactif, tandis que l'amélioration des processus de gestion des risques de sécurité tend à être un processus proactif. Améliorer les processus de l'État afin qu'ils soutiennent mieux la gestion des risques de sécurité permet d'identifier et de maîtriser les dangers avant que ceux-ci ne se manifestent sous la forme de résultats négatifs.

Atteindre l'ALoSP

8.5.5.13 La performance de sécurité d'un État telle qu'indiquée par ses SPI et ses SPT montre l'ALoSP atteint. Si aucune des SPT n'a été atteinte, une évaluation sera peut-être nécessaire pour mieux comprendre pourquoi et pour déterminer quelles actions devraient être prises. Il se peut que :

a) les cibles n'aient pas été atteignables ou réalistes ;

b) les actions entreprises pour atteindre la cible n'aient pas été appropriées ou se soient écartées de leur intention d'origine (dérive pratique) ;

c) des modifications d'autres priorités des risques de sécurité aient redirigé des ressources vers d'autres fins que la réalisation d'une cible particulière ;

d) des risques émergents soient apparus qui n'avaient pas été envisagés quand les cibles ont été fixées.

8.5.5.14 Lorsque des cibles n'ont pas été atteintes, il faudra comprendre pourquoi, et la direction devra décider si l'amélioration de la sécurité est suffisante même si la cible n'a pas été atteinte et quelles actions subséquentes seront requises. Pour ce faire, il faudra peut-être réaliser des analyses supplémentaires, susceptibles d'identifier certains facteurs de risque qui n'ont pas été traités ou certaines mesures d'atténuation des risques en place qui s'avèrent inefficaces.

8.5.6 Gestion du changement : point de vue de l'État

8.5.6.1 L'Annexe 19 n'exige pas explicitement que les États établissent des activités formelles de gestion du changement dans le cadre de leur PNS. Toutefois, les changements sont un fait omniprésent dans le système aéronautique contemporain. Lorsque des changements sont introduits dans un système, le bilan des risques de sécurité établi pour le système change. Des changements peuvent introduire des dangers susceptibles d'avoir une incidence sur l'efficacité des moyens de défense existants, ce qui pourrait générer un nouveau risque ou modifier des risques de sécurité existants. Les États devraient évaluer et gérer l'incidence du changement sur leurs systèmes aéronautiques.

8.5.6.2 Un PNS devrait instaurer des procédures pour évaluer l'incidence des changements au niveau de l'État. Les procédures devraient permettre à l'État d'identifier de façon proactive l'incidence que le changement apporté au système aéronautique aura sur la sécurité avant sa mise en œuvre, et de planifier et exécuter de façon structurée les changements proposés.

8.5.6.3 Une fois les changements planifiés, l'État devrait analyser l'incidence de ces changements sur le système existant et, en utilisant le processus de GRS existant, analyser, évaluer et, si nécessaire, atténuer tout risque de sécurité nouveau ou modifié. Aucune opération ne devrait avoir lieu dans un système ou un contexte opérationnel modifié tant que tous les risques de sécurité n'ont pas été évalués.

8.5.6.4 L'État sera confronté à deux types de changement dans le cadre de son PNS : les changements organisationnels (p. ex. une réattribution des responsabilités ou une restructuration au sein des autorités aéronautiques nationales) et les changements opérationnels (p. ex. un changement d'utilisation de l'espace aérien). La gestion des changements dans le cadre du PNS devrait se concentrer sur les changements qui pourraient avoir une incidence significative sur la capacité de l'État à remplir ses obligations légales (changements de processus) et sur les capacités de gestion de la sécurité de l'État. Elle pourrait inclure une combinaison de changements des processus et de changements opérationnels.

8.5.6.5 Voici une énumération, non limitative, de changements pouvant avoir une incidence significative sur les risques de sécurité de l'État :

a) réorganisation des autorités aéronautiques de l'État (y compris réduction des effectifs) ;

b) changements des processus du PNS, y compris changements de méthodologie tels que SRBS, GRS et processus d'assurance de la sécurité ;

c) changements de l'environnement réglementaire, tels que changements des politiques, programmes et réglementations de sécurité existants de l'État ;

d) changements dans l'environnement d'exploitation, tels que l'introduction de nouvelles technologies, changements touchant l'infrastructure, les équipements et les services ;

e) évolution rapide du secteur (expansion, contraction, transformation) et son incidence potentielle sur les capacités de l'État affectées à la supervision et au suivi des performances.

8.5.6.6 Il est fondamental de communiquer les changements pour assurer l'efficacité de la gestion des changements. Il est essentiel que le personnel concerné par ces changements au sein de l'État et du ou des prestataires de services affectés soit bien conscient du changement, du moment où il se produit et de ses incidences.

8.6 COMPOSANT 4 : PROMOTION DE LA SÉCURITÉ PAR L'ÉTAT

8.6.1 Du point de vue de l'État, la nécessité de mettre en œuvre des activités internes et externes de promotion de la sécurité est établie dans l'Annexe 19 en tant qu'un des composants des responsabilités des États en matière de gestion de la sécurité. Sur le plan interne, les AAC et autres autorités de l'aviation participant au PNS devraient établir des mécanismes pour fournir des informations de sécurité pertinentes à leur personnel pour favoriser le développement d'une culture qui encourage un PNS effectif et efficient. La communication des politiques de sécurité, plans de sécurité, ainsi que d'autres documents importants du PNS peut aussi améliorer la prise de conscience et la collaboration parmi le personnel, de sorte que les processus de gestion de la sécurité mis en place par les États restent efficaces.

8.6.2 L'amélioration de la performance de sécurité au sein d'un État ou d'un secteur aéronautique spécifique est hautement tributaire de sa culture de la sécurité. Les actions liées à la gestion de la sécurité tendent à être plus efficaces lorsque l'organisation a une culture positive de la sécurité. Lorsqu'ils sont visiblement soutenus par la haute direction et par les cadres intermédiaires, les employés en première ligne tendent à avoir un sens de la responsabilité partagée dans la réalisation de leurs objectifs de sécurité.

8.6.3 Par son importance, le besoin de communication se classe en tête des actions à mener pour améliorer la culture de la sécurité au sein d'un système aéronautique. En communiquant sans cesse ses priorités, ses bonnes pratiques, ses risques qui apparaissent nettement dans une opération particulière, l'État peut favoriser une culture positive de la sécurité et maximiser son potentiel d'atteindre ses objectifs de sécurité, que ce soit parmi les professionnels des AAC ou parmi les prestataires de services. De plus amples informations sur la culture de la sécurité figurent au Chapitre 3.

8.6.4 Une fois que les employés prennent à cœur leurs responsabilités en matière de performance de sécurité et les comprennent, on s'attend à ce qu'ils cherchent activement des moyens et des informations utilisables pour assumer avec efficacité leurs responsabilités de garantir une aviation sûre. C'est donc l'occasion de donner à la promotion de la sécurité un rôle clé dans la gestion de la sécurité. Sur le plan externe, l'établissement de canaux de communication avec les prestataires de services devrait permettre le partage des leçons tirées, des bonnes pratiques et des SPI et la fourniture d'informations sur des risques de sécurité spécifiques. Cela devrait soutenir la mise en œuvre de pratiques de gestion de la sécurité au sein des prestataires de services, ce qui devrait appuyer le développement d'une culture positive de la sécurité parmi des organisations similaires. De plus, le consentement d'efforts réguliers de communication avec les prestataires de services peut accroître la sensibilisation générale aux problèmes de sécurité de l'aviation et peut encourager un renforcement de la collaboration pour identifier des initiatives d'amélioration de la sécurité.

8.6.5 Lorsque des États prennent des décisions ou mènent des actions en vue d'améliorer la sécurité de l'aviation (p. ex. en établissant des réglementations ou en mettant en œuvre des changements dans leurs méthodes de surveillance), il est aussi important qu'ils communiquent tant en interne qu'avec l'extérieur. Cela peut renforcer la

perception de l'engagement de l'État dans l'ensemble de la communauté aéronautique, ce qui peut, à son tour, contribuer à la réalisation des objectifs de sécurité de l'État.

8.6.6 Beaucoup de ressources et d'outils sont disponibles pour aider les États à mettre en place des activités de promotion de la sécurité. Une façon de structurer les nombreuses activités de promotion qu'un État peut mener consiste à établir un plan de communication. Un tel plan pourrait inclure, au minimum, la cartographie des membres de la communauté aéronautique qui sont intéressés, les messages et informations transmis à chacun des groupes et les moyens par lesquels ces informations seront transmises. Le plan de communication peut aussi servir de feuille de route pour aider l'AAC à développer avec efficacité la capacité et les canaux pour communiquer avec ces publics internes et externes. Ces efforts peuvent contribuer à aider les États à développer une culture de la sécurité ainsi qu'à fournir les données nécessaires et les outils requis pour une gestion fructueuse de la sécurité, du point de vue tant des États que des prestataires de services.

8.6.7 Certaines informations peuvent être communiquées par le biais de bulletins et publications moins formels sur les réseaux sociaux, tandis que d'autres seront plutôt à traiter dans des réunions ou séminaires spécifiques. Il appartient à l'État de mettre en œuvre les canaux et médias adéquats de promotion de la sécurité qu'il estime à même de produire les meilleurs résultats pour développer une culture positive de la sécurité au sein de l'État et concrétiser, à terme, un PNS efficace et un système d'aviation civile plus sûr au sein de l'État.

8.6.8 Communication interne et diffusion des informations

Note.— Les informations de sécurité provenant de systèmes de compte rendu volontaire en matière de sécurité devront être protégées, sauf si un principe régissant les dérogations s'applique. Cette remarque peut être étendue aux informations de sécurité provenant d'un système de compte rendu obligatoire. Voir le Chapitre 7 pour plus de détails sur la protection des données de sécurité, des informations de sécurité et des sources connexes.

8.6.8.1 Les activités et publications visant à promouvoir la sécurité peuvent aussi améliorer la coordination et la collaboration entre différentes organisations participant à la supervision de la sécurité au sein de l'État. Le document du PNS et ses politiques nationales connexes de sécurité et d'application des lois sont indispensables pour parvenir à intégrer la formation, la communication et la diffusion des informations qui y sont associées. Les autorités de réglementation de l'État responsables des différents secteurs de l'aviation ainsi que d'autres entités administratives indépendantes telles que l'AIA devraient adopter une approche intégrée de leurs rôles respectifs dans la promotion de la sécurité entreprise par l'État. Les États devraient établir des canaux de communication formels entre les membres du groupe de coordination du PNS (entités de l'État contribuant à mettre en œuvre le PNS et à le tenir à jour).

8.6.8.2 Du point de vue de l'exploitation, il est important que les stratégies d'exploitation exposées dans le PNS, y compris les exigences harmonisées concernant les SGS et le suivi des différents prestataires de services, soient partagées, communiquées et coordonnées entre les autorités aéronautiques de l'État. Un canal de communication ouvert peut éviter la création d'exigences conflictuelles concernant les SGS ou de critères d'acceptation divergents pour différents secteurs de l'aviation.

8.6.8.3 Voici des exemples d'informations que les États devraient aborder dans leurs communications et activités de diffusion internes :

a) documentation du PNS, politiques et procédures ;

b) SPI ;

c) informations sur la performance de sécurité du secteur ;

d) profils de risques liés à la sécurité organisationnelle du secteur ;

e) communication de la responsabilité en matière de sécurité du système ;

f) leçons tirées des accidents et incidents ;

g) concepts et meilleures pratiques de gestion de la sécurité.

8.6.8.4 Lorsque des prestataires de services sont approuvés par plus d'un État, il est indispensable d'avoir des lignes ouvertes pour les communications de sécurité.

8.6.8.5 Les organisations de l'État peuvent adopter plusieurs moyens pour transmettre des communications de sécurité en interne, notamment des lettres d'informations, bulletins, dépliants, publications, séminaires, réunions, formations, sites web, listes de publipostage, publications sur les médias sociaux, discussions dans des groupes de collaboration.

8.6.8.6 Lorsqu'elle évalue quel type de médias devrait être utilisé pour transmettre un message particulier, l'organisation devrait évaluer lequel est le plus approprié pour chaque message et son public cible. Les documents du PNS peuvent être affichés sur un site web déjà accessible pour le personnel, lorsque celui-ci en a besoin. D'autres informations, telles que les leçons tirées et les meilleures pratiques, peuvent se prêter à une publication dans un bulletin ou une lettre d'information périodique.

8.6.8.7 Mener des campagnes dans de multiples médias pour aborder une préoccupation ou un danger particuliers peut être efficace pour renforcer la sensibilisation au problème et changer l'attitude du personnel.

8.6.9 Communication externe et diffusion d'informations de sécurité

8.6.9.1 L'État devrait créer des plates-formes ou des médias appropriés de communication pour faciliter la mise en œuvre des SGS et améliorer la culture de la sécurité dans l'ensemble du système.

8.6.9.2 Quand ils communiquent et diffusent des informations de sécurité en externe avec l'industrie aéronautique, outre les éléments présentés dans la section précédente, les États devraient aussi envisager d'inclure :

a) des éléments indicatifs pour la mise en œuvre des SGS ;

b) l'importance du compte rendu ;

c) l'identification des formations à la sécurité disponibles pour la communauté aéronautique ;

d) la promotion des échanges d'informations de sécurité :

1) avec et entre les prestataires de services ;

2) entre Les États.

8.6.9.3 La documentation du PNS de l'État et ses politiques de sécurité et d'application connexes devraient aussi être mises à la disposition des prestataires de services, selon les besoins.

8.6.9.4 Essentiellement, les mêmes médias d'appui utilisés pour les communications internes peuvent être utilisés pour les communications externes, pour autant que le contenu soit utile pour les deux publics cibles. Toutefois, pour les communications externes, une attention particulière peut être accordée à des solutions qui atteignent des publics plus vastes, telles que les médias sociaux, listes de publipostage, bulletins, séminaires, afin de créer au sein de l'industrie des communautés pour l'échange d'informations de sécurité, ce qui multiplie la portée des messages.

8.6.9.5 Les États devraient promouvoir l'établissement de réseaux de partage ou d'échange d'informations de sécurité au sein de la communauté aéronautique, à moins que les lois nationales s'y opposent.

8.7 MISE EN ŒUVRE DU PNS

Comme pour la mise en œuvre de tout projet majeur, la mise en œuvre du PNS exige la réalisation de beaucoup de tâches et de sous-tâches selon un calendrier prédéterminé. Le nombre de tâches ainsi que la portée de chaque tâche dépendent de la maturité du système de supervision de la sécurité de l'État. Dans la plupart des États, plusieurs organisations et entités participent à l'élaboration et à la mise en œuvre d'un PNS. L'élaboration d'un plan de mise en œuvre peut contribuer à faciliter ce processus. La présente section décrit les étapes depuis la rédaction d'une description complète du système, les considérations liées à la variabilité, l'exécution d'une analyse des lacunes, jusqu'à l'élaboration d'un plan de mise en œuvre qui inclut la garantie de l'établissement d'une base solide pour le PNS. Cette section aborde aussi l'évaluation continue de la maturité d'un PNS.

8.7.1 Description du système d'aviation civile de l'État et considérations relatives à la variabilité

8.7.1.1 La compréhension de la taille et de la complexité du système aéronautique d'un État et des interactions entre les éléments est fondamentale pour planifier le PNS. Les États sont tenus de mettre en œuvre un PNS mais la façon dont ils respecteront les exigences dépendra de la taille et de la complexité du système aéronautique. De plus amples informations sur la variabilité sont données au Chapitre 1.

8.7.1.2 Le PNS devra aussi tenir compte du nombre de prestataires de services dans chaque domaine de l'aviation, de leur taille et complexité et de l'environnement régional. Les États ayant un petit nombre de prestataires de services devraient envisager d'établir des partenariats régionaux. Les partenariats régionaux avec d'autres États ou par l'intermédiaire de RSOO et le partage des leçons tirées et des informations sur les risques de sécurité réduiront au minimum l'incidence tout en maximisant les avantages de la mise en œuvre du PNS.

8.7.1.3 Les États devraient décrire le système d'aviation et les diverses autorités aéronautiques nationales dans une description du système d'aviation civile. Celle-ci devrait comporter un aperçu général des structures et interfaces organisationnelles. Cela fait partie du processus de planification de la mise en œuvre du PNS. Une telle description devrait notamment aborder les éléments suivants :

a) la structure du cadre réglementaire existant pour l'aviation, y compris les diverses autorités aéronautiques de l'État ;

b) les rôles et responsabilités des diverses autorités de réglementation en matière de gestion de la sécurité ;

c) une plate-forme ou un mécanisme de coordination du PNS entre les organisations ;

d) un mécanisme d'examen interne au niveau de l'État et au sein de chaque organisation.

8.7.2 Analyse des lacunes du PNS et plan de mise en œuvre

Analyse des lacunes du PNS

8.7.2.1 Une analyse des lacunes devrait être menée avant l'élaboration d'un plan de mise en œuvre du PNS. L'analyse des lacunes vise à donner une compréhension détaillée des différences entre les structures et processus existants de l'État et ceux qu'exige une mise en œuvre efficace du PNS dans l'État. Dans beaucoup d'États, l'analyse

des lacunes révèle qu'il existe déjà des capacités considérables de gestion de la sécurité. La difficulté consiste généralement à affiner, réaligner et renforcer des capacités existantes. Les éléments ou processus identifiés comme nécessitant une action constituent la base du plan de mise en œuvre du PNS.

Base du PNS

8.7.2.2 Il est essentiel que les États établissent une base mature pour soutenir une mise en œuvre efficace du PNS. Les objectifs du GASP appellent les États à mettre progressivement en œuvre des systèmes efficaces de supervision de la sécurité, des PNS et les capacités avancées de gestion de la sécurité, nécessaires pour soutenir les systèmes d'aviation futurs. Cette base couvre les aspects du système de supervision de la sécurité qui sont nécessaires pour soutenir une approche plus fondée sur les performances.

8.7.2.3 Les données collectées au titre du Programme universel OACI d'audits de supervision de la sécurité (USOAP) peuvent être utilisées pour identifier les carences dans cette base. La première étape de la mise en œuvre du PNS devrait s'attacher à résoudre toute insuffisance dans les réponses aux questions de protocole USOAP relatives aux problèmes liés à une mise en œuvre efficace du PNS (p. ex. systèmes de compte rendu obligatoire).

Plan de mise en œuvre du PNS

8.7.2.4 La mise en œuvre du PNS vise à progressivement renforcer les processus SSO et processus de gestion de la sécurité existants. Les tâches/sous-tâches appropriées sont priorisées et documentées dans un plan d'action. Un plan de mise en œuvre du PNS ainsi que le document (exposition) de haut niveau du PNS fournissent des « bases » qui guident le cheminement de l'État vers un PNS efficace et vers une amélioration continue de la performance de sécurité. Ces deux documents clés devraient être faciles d'accès pour tout le personnel pertinent afin de garantir que toute personne concernée ait connaissance du PNS et de ses plans de mise en œuvre.

8.7.3 Évaluation de la maturité du PNS

Contexte et objet

8.7.3.1 L'évaluation de la maturité du PNS devrait être réalisée à l'aide d'un outil qui reflète les SARP et éléments indicatifs de l'OACI, outil mis au point par l'État pour répondre à ses besoins. Cet outil devrait être utilisé par les États pour effectuer des audits internes en vue de l'amélioration continue du PNS. Il devrait aussi être cité en référence par l'OACI et d'autres entités externes, selon le cas. Cet outil devrait reposer sur une série de questions (ou d'attentes) pouvant être utilisées par l'État pour évaluer l'efficacité de son PNS. Des interactions, telles que des discussions et des entretiens en face à face, avec un échantillon de toutes les parties intéressées, seront utiles pour l'évaluation de la maturité du PNS. Cet outil devrait être souple et tenir compte de la taille et de la complexité du système d'aviation de l'État.

Évaluation

8.7.3.2 Une fois les aspects fondamentaux du PNS en place, une évaluation de la documentation peut être réalisée. Cette évaluation vise à révéler si les attentes du PNS pour ce qui est de la conformité et de la performance sont présentes et appropriées. Des données factuelles devraient être collectées à l'appui de l'évaluation. À un stade ultérieur, il est possible d'évaluer le PNS pour comprendre s'il fonctionne bien et s'il réalise ses objectifs avec efficacité. L'efficacité est atteinte lorsque les extrants produisent à chaque fois le résultat souhaité. Normalement, c'est une équipe ayant des compétences appropriées et des savoir-faire techniques en gestion de PNS qui mène l'évaluation et collecte les preuves. Il est important de structurer l'évaluation de façon à permettre une interaction avec plusieurs personnes à des niveaux différents de l'organisation, afin de déterminer l'efficacité dans l'ensemble de l'organisation. Par exemple,

déterminer dans quelle mesure la politique de sécurité a été promulguée et comprise par le personnel exigera une interaction avec un échantillon des diverses catégories de personnel.

Suivi permanent et amélioration continue

8.7.3.3 L'État peut utiliser le même outil pour évaluer l'efficacité de son PNS pendant le processus de suivi permanent et d'amélioration continue. Cette évaluation identifiera probablement des changements apportés au système aéronautique. Dans la plupart des États, il faudra du temps pour mettre en œuvre le PNS et plusieurs années pour que celui-ci atteigne un niveau de maturité où tous les éléments fonctionnent efficacement. La Figure 8-5 illustre les différents niveaux de maturité du PNS à mesure que l'État avance dans la mise en œuvre et développe son PNS.

8.7.3.4 Une évaluation du PNS peut être menée à diverses étapes, en examinant initialement si des éléments clés sont présents et appropriés. À un stade ultérieur, il est possible d'évaluer le PNS pour comprendre s'il fonctionne bien et s'il réalise ses objectifs avec efficacité. Les États peuvent continuer à effectuer des évaluations périodiques pour appuyer l'amélioration continue sur la voie de l'excellence.

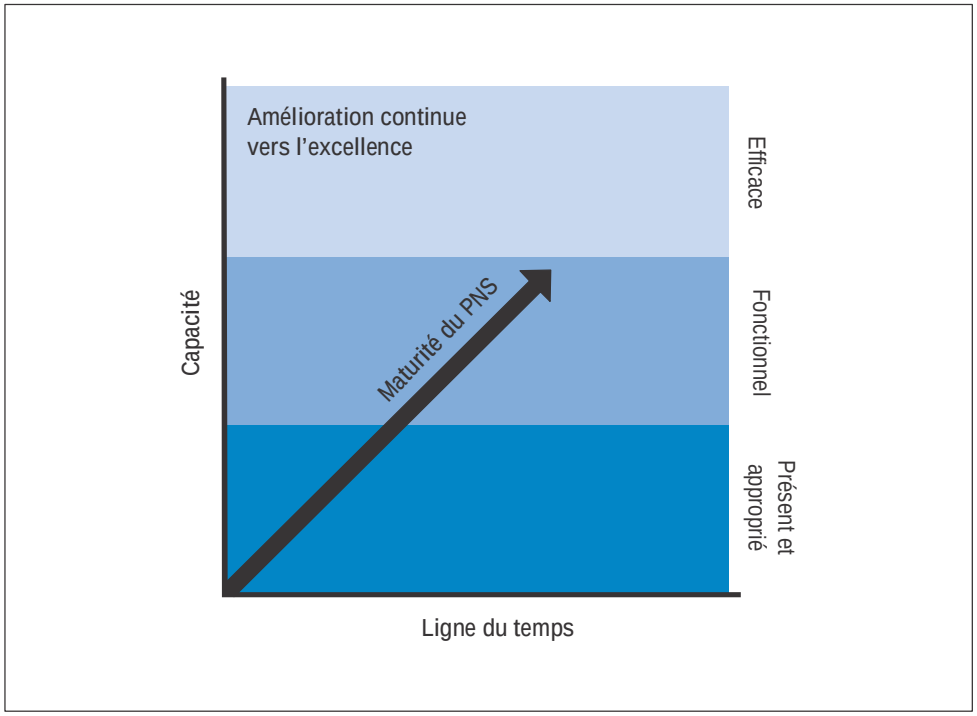

Figure 8-5. Trajet de maturation d'un PNS

Chapitre 9

SYSTÈMES DE GESTION DE LA SÉCURITÉ (SGS)

9.1 INTRODUCTION

9.1.1 Le présent chapitre donne aux prestataires de services des orientations sur la mise en œuvre d'un cadre pour un SGS conformément à l'Annexe 19, et aux États, des orientations sur la supervision des SGS.

9.1.2 L'objet d'un SGS est de donner aux prestataires de services une approche systématique pour gérer la sécurité. Un SGS est conçu pour améliorer en continu la performance de sécurité par l'identification des dangers, la collecte et l'analyse des données de sécurité et des informations de sécurité et l'évaluation continue des risques de sécurité. Le SGS tente d'atténuer proactivement les risques de sécurité avant qu'ils ne provoquent des accidents et des incidents d'aviation. Il permet aux prestataires de services de gérer efficacement leurs activités, leur performance de sécurité et leurs ressources, tout en gagnant une meilleure compréhension de leur contribution à la sécurité de l'aviation. Un SGS efficace prouve aux États la capacité du prestataire de services à gérer les risques de sécurité et permet une gestion efficace de la sécurité à l'échelon de l'État.

9.1.3 Les exploitants de l'aviation générale internationale devraient déterminer les critères des SGS pour les aéronefs qu'ils exploitent, tels qu'établis par l'État d'immatriculation, et garantir que leur SGS est acceptable pour l'État d'immatriculation. Pour faciliter l'acceptabilité du SGS, les exploitants de l'aviation générale internationale devraient demander à l'État d'immatriculation si l'utilisation d'un code de pratique de l'industrie est autorisée.

9.1.4 Les exploitants d'aéronefs lourds ou à turboréacteurs exploités sous de multiples États d'immatriculation en vertu d'un permis d'exploitation aérienne (AOC) délivré conformément à l'Annexe 6, Partie 1, sont considérés comme des prestataires de services et, par conséquent, leur SGS doit être rendu acceptable pour l'État de l'exploitant.

9.2 CADRE POUR UN SGS

9.2.1 L'Annexe 19 spécifie le cadre pour la mise en œuvre et la tenue à jour d'un SGS. Tous les éléments du cadre pour un SGS sont d'application, quelles que soient la taille et la complexité du prestataire de services. La mise en œuvre devrait être adaptée à l'organisation et à ses activités.

9.2.2 Le cadre pour un SGS de l'OACI est constitué des quatre composants et douze éléments suivants :

Tableau 10. Composants et éléments du cadre pour un SGS de l'OACI

COMPOSANT	*ÉLÉMENT*
1. Politique et objectifs de sécurité	1.1 Engagement de la direction
	1.2 Obligation de rendre compte et responsabilités en matière de sécurité
	1.3 Nomination du personnel clé chargé de la 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 Suivi et mesure de la performance de sécurité
	3.2 La gestion du changement
	3.3 Amélioration continue du SGS
4. Promotion de la sécurité	4.1 Formation et sensibilisation
	4.2 Communication en matière de sécurité

9.3 COMPOSANT 1 : POLITIQUE ET OBJECTIFS DE SÉCURITÉ

9.3.1 Le premier composant du cadre pour un SGS se concentre sur la création d'un environnement dans lequel la gestion de la sécurité peut être efficace. Il repose sur une politique et des objectifs de sécurité qui énoncent l'engagement de la haute direction envers la sécurité, ses buts et la structure organisationnelle d'appui.

9.3.2 L'engagement de la direction et le leadership dans le domaine de la sécurité sont indispensables pour la mise en œuvre d'un SGS efficace et sont affirmés dans la politique de sécurité et par l'établissement d'objectifs de sécurité. L'engagement de la direction envers la sécurité est démontré au moyen du processus décisionnel de la direction et de l'affectation des ressources ; ces décisions et actions devraient toujours être cohérentes avec la politique et les objectifs de sécurité afin d'encourager une culture positive de la sécurité.

9.3.3 La politique de sécurité devrait être élaborée et approuvée par la haute direction et doit être signée par le dirigeant responsable. Le personnel de sécurité clé et, le cas échéant, les instances représentatives du personnel (forums des employés, syndicats) devraient être consultés pour l'élaboration de la politique de sécurité et des objectifs de sécurité, afin de promouvoir un sens de la responsabilité partagée.

9.3.4 Engagement de la direction

Politique de sécurité

9.3.4.1 La politique de sécurité devrait être visiblement approuvée par la haute direction et par le dirigeant responsable. La notion d'« approbation visible » traduit le fait que l'appui actif de la direction à la politique de sécurité est rendu visible pour le reste de l'organisation. Cette visibilité peut être atteinte par tout moyen de communication et par l'alignement des activités sur la politique de sécurité.

9.3.4.2 Il incombe à la direction de communiquer la politique de sécurité dans l'ensemble de l'organisation, afin de garantir que tout le personnel comprenne cette politique de sécurité et travaille dans le respect de celle-ci.

9.3.4.3 Pour refléter l'engagement de l'organisation envers la sécurité, la politique de sécurité devrait comporter un engagement à :

a) améliorer en continu le niveau de performance de sécurité ;

b) promouvoir et maintenir une culture positive de la sécurité au sein de l'organisation ;

c) respecter toutes les exigences réglementaires applicables ;

d) fournir les ressources nécessaires pour livrer un produit ou un service sûr ;

e) garantir que la sécurité est une responsabilité première de tous les cadres ;

f) garantir que cette politique est comprise, mise en œuvre et maintenue à tous les niveaux.

9.3.4.4 La politique de sécurité devrait aussi faire référence au système de compte rendu en matière de sécurité, afin d'encourager des comptes rendus de problèmes de sécurité et d'informer le personnel au sujet de la politique disciplinaire appliquée lorsque des événements de sécurité ou des problèmes de sécurité sont signalés.

9.3.4.5 La politique disciplinaire est utilisée pour déterminer si une erreur ou une violation de règle a été commise, de sorte que l'organisation puisse établir si une mesure disciplinaire doit être prise. Pour garantir le traitement équitable des personnes concernées, il est essentiel que ceux qui ont la responsabilité d'établir s'il y a eu erreur ou violation aient les savoir-faire techniques requis pour tenir pleinement compte du contexte de l'événement.

9.3.4.6 Une politique relative à la protection des données de sécurité et des informations de sécurité, ainsi que des auteurs de comptes rendus, peut avoir un effet positif sur la culture du compte rendu. Le prestataire de services et l'État devraient autoriser l'anonymisation et l'agrégation des comptes rendus pour permettre la réalisation d'analyses de sécurité utiles ne nécessitant pas une implication du personnel ou de prestataires de services spécifiques. Étant donné que des événements majeurs peuvent être liés à des processus et procédures extérieurs au SGS du prestataire de services, l'autorité pertinente de l'État peut ne pas autoriser l'anonymisation précoce des comptes rendus dans toutes les circonstances. Néanmoins, une politique autorisant l'anonymisation appropriée des comptes rendus peut améliorer la qualité des données collectées.

Objectifs de sécurité

9.3.4.7 En tenant compte de sa politique de sécurité, le prestataire de services devrait aussi établir des objectifs de sécurité pour définir ce qu'il vise à atteindre au chapitre des résultats de sécurité. Les objectifs de sécurité devraient être des déclarations brèves, de haut niveau, relatives aux priorités de sécurité de l'organisation et ils devraient aborder les risques de sécurité les plus significatifs de l'organisation. Les objectifs de sécurité peuvent être inclus dans la politique de sécurité (ou documentés séparément), qui définit ce que l'organisation vise à atteindre en matière de sécurité. Les indicateurs de performance de sécurité (SPI) et les cibles de performance de sécurité (SPT) sont nécessaires pour le suivi de la réalisation de ces objectifs de sécurité et sont présentés plus en détail dans ce chapitre, sous le composant 3.

9.3.4.8 La politique de sécurité et les objectifs de sécurité devraient être revus périodiquement pour garantir qu'ils restent pertinents (un changement de dirigeant responsable requerrait leur révision, par exemple).

9.3.5 Obligation de rendre compte et responsabilités en matière de sécurité

Dirigeant responsable

9.3.5.1 Le dirigeant responsable, généralement le directeur général, est la personne qui a l'autorité ultime sur l'exploitation sûre de l'organisation. Le dirigeant responsable établit et promeut la politique de sécurité et les objectifs de sécurité qui insufflent la sécurité en tant que valeur organisationnelle fondamentale. Il devrait avoir le pouvoir de prendre des décisions au nom de l'organisation, avoir le contrôle des ressources tant financières qu'humaines, être responsable de garantir que des actions appropriées soient prises pour résoudre les problèmes de sécurité et gérer les risques de sécurité et il devrait être chargé de réagir en cas d'accidents et d'incidents.

9.3.5.2 Il peut être difficile pour le prestataire de services d'identifier la personne la plus appropriée pour occuper ce poste de dirigeant responsable, surtout dans de grandes organisations complexes ayant des entités multiples et des certificats, autorisations ou approbations multiples. Il importe que la personne sélectionnée occupe un poste au plus haut niveau de l'organisation, afin de garantir la prise de bonnes décisions stratégiques en matière de sécurité.

9.3.5.3 Le prestataire de services est tenu d'identifier le dirigeant responsable et d'attribuer la responsabilité de la performance de sécurité générale à un niveau de l'organisation ayant l'autorité nécessaire pour prendre des mesures afin de garantir l'efficacité du SGS. Les obligations spécifiques de rendre compte en matière de sécurité incombant à tous les membres de la direction devraient être définies et le rôle des membres de la direction dans le SGS devrait refléter la façon dont ces personnes peuvent contribuer à une culture positive de la sécurité. Les responsabilités, obligations de rendre compte et pouvoirs en matière de sécurité devraient être documentés et communiqués dans l'ensemble de l'organisation. Les obligations de rendre compte en matière de sécurité incombant aux gestionnaires devraient inclure l'affectation des ressources humaines, techniques, financières ou autres qui sont requises pour assurer une performance efficace et efficiente du SGS.

Note.— « Obligation de rendre compte » désigne une obligation qui ne peut pas être déléguée. « Responsabilité » désigne des fonctions et activités qui peuvent être déléguées.

9.3.5.4 Dans le cas où un SGS s'applique à plusieurs certificats, autorisations ou approbations différents qui font tous partie de la même entité juridique, il ne devrait y avoir qu'un seul dirigeant responsable. Si ce n'est pas possible, un dirigeant responsable distinct devrait être identifié pour chaque certificat, autorisation ou approbation de l'organisation et des lignes claires d'obligations de rendre compte devraient être définies ; il est aussi important d'identifier comment les obligations de rendre compte en matière de sécurité seront coordonnées.

9.3.5.5 Une des façons les plus efficaces d'associer visiblement le dirigeant responsable au processus est de lui faire présider des réunions de sécurité régulières à l'échelon de la direction. Étant donné que le dirigeant responsable assume la responsabilité ultime de la sécurité de l'organisation, sa participation active à ces réunions lui permet :

a) d'analyser les objectifs de sécurité ;

b) d'assurer le suivi de la performance de sécurité et de la réalisation des cibles de sécurité ;

c) de prendre des décisions en matière de sécurité en temps utile ;

d) d'affecter les ressources appropriées ;

e) de demander des comptes aux gestionnaires au sujet des responsabilités en matière de sécurité, de la performance de sécurité et des calendriers de mise en œuvre ;

f) d'être perçu par tout le personnel comme un dirigeant qui s'intéresse à la sécurité et est aux commandes en matière de sécurité.

9.3.5.6 Le dirigeant responsable ne participe généralement pas aux activités quotidiennes de l'organisation ou à la résolution des problèmes survenant sur les lieux de travail et il devrait s'assurer qu'il existe une structure organisationnelle appropriée pour gérer et exécuter le SGS. La responsabilité de la gestion de la sécurité est souvent déléguée à l'équipe de la haute direction et à d'autres membres clés du personnel en charge de la sécurité. Bien que la responsabilité du fonctionnement du SGS au quotidien puisse être déléguée, le dirigeant responsable ne peut déléguer l'obligation de rendre compte du système ni les décisions relatives aux risques de sécurité. Par exemple, les obligations suivantes de rendre compte en matière de sécurité ne peuvent être déléguées :

a) veiller à ce que les politiques de sécurité soient appropriées et communiquées ;

b) veiller à affecter les ressources nécessaires (financement, personnel, formation, acquisition) ;

c) fixer les limites acceptables pour les risques de sécurité et affecter les ressources requises pour les mesures nécessaires de maîtrise des risques.

9.3.5.7 Il est approprié que le dirigeant responsable ait les obligations suivantes de rendre compte en matière de sécurité :

a) fournir des ressources financières et humaines suffisantes pour une mise en œuvre correcte d'un SGS efficace ;

b) promouvoir une culture positive de la sécurité ;

c) établir et promouvoir la politique de sécurité ;

d) établir les objectifs de sécurité de l'organisation ;

e) garantir que le SGS est correctement mis en œuvre et qu'il fonctionne conformément aux exigences ;

f) veiller à l'amélioration continue du SGS.

9.3.5.8 Les pouvoirs du dirigeant responsable incluent, mais sans s'y limiter, l'autorité ultime :

a) pour la résolution de tous les problèmes de sécurité ;

b) pour les opérations menées sous certificat, autorisation ou approbation de l'organisation, y compris le pouvoir d'arrêter l'opération ou l'activité.

9.3.5.9 Le pouvoir de prendre des décisions concernant la tolérabilité des risques de sécurité devrait être défini. À cet égard, il convient de déterminer qui peut prendre des décisions sur l'acceptabilité de risques et qui a le pouvoir d'accepter qu'un changement puisse être mis en œuvre. Ce pouvoir peut être attribué à une personne, à un poste de direction ou à un comité.

9.3.5.10 Le pouvoir de prendre des décisions quant à la tolérabilité des risques de sécurité devrait être proportionnel aux pouvoirs généraux du gestionnaire en matière de prise de décisions et d'affectation des ressources. Un cadre d'un niveau inférieur (ou un groupe de gestion) peut être autorisé à prendre des décisions quant à la tolérabilité, jusqu'à un certain niveau. Les niveaux de risque qui dépassent les pouvoirs du gestionnaire doivent être renvoyés pour examen à un niveau de direction supérieur ayant des pouvoirs plus étendus.

Obligation de rendre compte et responsabilités

9.3.5.11 Il faudrait définir clairement les obligations de rendre compte et les responsabilités de l'ensemble du personnel, cadres dirigeants et collaborateurs, qui participent à des tâches liées à la sécurité à l'appui d'une fourniture de produits et opérations sûrs. Les responsabilités en matière de sécurité devraient se concentrer sur la contribution des membres du personnel à la performance de sécurité de l'organisation (extrants liés à la sécurité organisationnelle). La gestion de la sécurité est une fonction fondamentale ; à ce titre, chaque cadre supérieur est dans une certaine mesure associé au fonctionnement du SGS.

9.3.5.12 Toutes les obligations de rendre compte, toutes les responsabilités et tous les pouvoirs devraient être énoncés dans la documentation du SGS du prestataire de services et devraient être communiqués dans l'ensemble de l'organisation. Les obligations de rendre compte et les responsabilités de chaque cadre supérieur font partie intégrante de leurs descriptions de fonctions. Celles-ci devraient aussi aborder les différentes fonctions de gestion de la sécurité entre cadres hiérarchiques et gestionnaire de la sécurité (voir § 9.3.6 pour de plus amples informations).

9.3.5.13 Les lignes d'obligations de rendre compte en matière de sécurité dans l'ensemble de l'organisation et leur définition dépendront du type et de la complexité de l'organisation et des méthodes de communication privilégiées par celle-ci. Généralement, les obligations de rendre compte et les responsabilités en matière de sécurité seront reflétées dans les organigrammes, les documents définissant les responsabilités des services et les descriptions des fonctions et des rôles du personnel.

9.3.5.14 Le prestataire de services devrait s'attacher à éviter les conflits d'intérêts entre les responsabilités en matière de sécurité et les autres responsabilités organisationnelles des membres du personnel. Il devrait attribuer les obligations de rendre compte et les responsabilités liées au SGS de façon à réduire au minimum les chevauchements et/ou lacunes.

Obligation de rendre compte et responsabilités vis-à-vis d'organisations externes

9.3.5.15 Un prestataire de services est responsable de la performance de sécurité d'organisations externes lorsqu'il existe une interface avec le SGS. Le prestataire de services peut devoir rendre compte de la performance de sécurité de produits ou services fournis par des organisations externes qui soutiennent ses activités, même si ces organisations externes ne sont pas tenues d'avoir un SGS. Il est essentiel que le SGS du prestataire de services ait une interface avec les systèmes de sécurité de toute organisation externe qui contribue à la fourniture sûre de ses produits ou services.

9.3.6 Nomination du personnel clé chargé de la sécurité

9.3.6.1 Pour garantir une mise en œuvre et un fonctionnement efficaces du SGS, il est essentiel de désigner une ou plusieurs personnes compétentes pour assumer le rôle de gestionnaire de la sécurité. Le gestionnaire de la sécurité peut porter des titres différents. Aux fins du présent manuel, le titre générique « gestionnaire de la sécurité » désigne la fonction, pas nécessairement l'individu. La personne qui assume la fonction de gestionnaire de la sécurité rend compte au dirigeant responsable en ce qui concerne la performance du SGS et la fourniture de services de sécurité aux autres services de l'organisation.

9.3.6.2 Le gestionnaire de la sécurité conseille le dirigeant responsable et les cadres hiérarchiques sur les matières 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 des membres externes de la communauté aéronautique. Les fonctions de gestionnaire de la sécurité incluent, sans s'y limiter, les activités suivantes :

a) gérer le plan de mise en œuvre du SGS au nom du dirigeant responsable (lors de la mise en œuvre initiale) ;

b) effectuer/faciliter l'identification des dangers et l'analyse des risques de sécurité ;

c) assurer le suivi des mesures correctrices et évaluer leurs résultats ;

d) fournir des rapports périodiques sur la performance de sécurité de l'organisation ;

e) tenir à jour la documentation et les dossiers du SGS ;

f) planifier et faciliter la formation du personnel à la sécurité ;

g) donner des conseils indépendants sur les questions de sécurité ;

h) assurer le suivi des préoccupations en matière de sécurité dans l'industrie aéronautique et de leur incidence perçue sur les opérations de l'organisation destinées à fournir des produits et services ;

i) assurer (au nom du dirigeant responsable) la coordination et la communication sur les questions relatives à la sécurité avec l'AAC de l'État et d'autres autorités de l'État, selon les nécessités.

9.3.6.3 Dans la plupart des organisations, une personne est désignée gestionnaire de la sécurité. Selon la taille, la nature et la complexité de l'organisation, le gestionnaire de la sécurité peut avoir une fonction exclusive ou son rôle peut être combiné à d'autres tâches. De plus, certaines organisations doivent parfois attribuer ce rôle à un groupe de personnes. L'organisation doit s'assurer que l'option choisie n'entraîne pas de conflits d'intérêts. Dans la mesure du possible, le gestionnaire de la sécurité ne devrait pas être directement associé à la fourniture de produits ou de services mais devrait avoir une connaissance pratique de ces produits ou services. La désignation devrait aussi tenir compte de conflits d'intérêts potentiels avec d'autres tâches et fonctions. De tels conflits d'intérêts pourraient inclure :

a) une concurrence pour le financement (p. ex. si le directeur financier est le gestionnaire de la sécurité) ;

b) des priorités conflictuelles pour l'affectation des ressources ;

c) un scénario où le gestionnaire de la sécurité a un rôle opérationnel et la capacité d'évaluer l'efficacité du SGS pour les activités opérationnelles auxquelles il participe.

9.3.6.4 Dans les cas où la fonction est attribuée à un groupe de personnes (p. ex. lorsque des prestataires de services étendent leur SGS à de multiples activités), une de ces personnes devrait être désignée gestionnaire de la sécurité « principal », afin de maintenir une ligne de compte rendu directe et univoque vers le dirigeant responsable.

9.3.6.5 Les compétences d'un gestionnaire de la sécurité devraient inclure, sans s'y limiter, les éléments suivants :

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

b) une expérience opérationnelle du produit ou du service fourni par l'organisation ;

c) des compétences techniques pour comprendre les systèmes qui sous-tendent les opérations ou le produit/service fourni ;

d) des compétences interpersonnelles ;

e) des aptitudes d'analyse et de résolution des problèmes ;

f) des aptitudes à gérer des projets ;

g) des aptitudes en communication orale et écrite ;

h) une compréhension des facteurs humains.

9.3.6.6 Selon la taille, la nature et la complexité de l'organisation, du personnel supplémentaire peut aider le gestionnaire de la sécurité. Le gestionnaire de la sécurité et le personnel d'appui sont responsables d'assurer la collecte et l'analyse rapides des données de sécurité et la diffusion appropriée, au sein de l'organisation, des informations de sécurité qui y sont associées, afin que des décisions sur les risques de sécurité et des mesures de maîtrise de ces risques puissent être prises.

9.3.6.7 Les prestataires de services devraient créer des comités de sécurité appropriés pour soutenir les fonctions liées au SGS dans toute l'organisation. À cet égard, ils devraient notamment déterminer la composition du comité de sécurité et la fréquence de ses réunions.

9.3.6.8 Le comité de sécurité du niveau le plus élevé, parfois appelé commission d'examen de la sécurité (SRB), inclut le dirigeant responsable et les cadres supérieurs, le gestionnaire de la sécurité y participant à titre consultatif. La SRB est stratégique et traite des questions de haut niveau liées aux politiques de sécurité, à l'affectation des ressources et à la performance de l'organisation. La SRB surveille :

a) l'efficacité du SGS ;

b) la mise en œuvre, en temps utile, des mesures de maîtrise des risques de sécurité nécessaires ;

c) la performance de sécurité par rapport à la politique et aux objectifs de sécurité de l'organisation ;

d) l'efficacité générale des stratégies d'atténuation des risques de sécurité ;

e) l'efficacité des processus de gestion de la sécurité de l'organisation qui soutiennent :

1) la priorité organisationnelle explicite accordée à la gestion de la sécurité ;

2) la promotion de la sécurité dans l'ensemble de l'organisation.

9.3.6.9 Une fois qu'une direction stratégique a été élaborée par le comité de sécurité de haut niveau, la mise en œuvre de stratégies de sécurité devrait être coordonnée dans l'ensemble de l'organisation. Pour ce faire, des groupes d'action pour la sécurité (SAG), plus centrés sur le côté opérationnel, peuvent être créés. Les SAG se composent normalement de cadres et de personnel de première ligne et sont présidés par un directeur désigné. Les SAG sont des entités tactiques qui traitent de problèmes spécifiques de mise en œuvre sur la base des stratégies élaborées par la SRB. Les SAG :

a) suivent la performance de sécurité opérationnelle dans leurs secteurs fonctionnels au sein de l'organisation et veillent à ce que des activités de GRS appropriées soient exécutées ;

b) analysent les données de sécurité disponibles, déterminent la mise en œuvre de stratégies appropriées de maîtrise des risques de sécurité et veillent à fournir des rétro-informations au personnel ;

c) évaluent quelle incidence l'introduction de changements opérationnels ou de nouvelles technologies a sur la sécurité ;

d) coordonnent la mise en œuvre de toute action liée à des mesures de maîtrise des risques de sécurité et garantissent la prise rapide de mesures ;

e) examinent l'efficacité de mesures spécifiques de maîtrise des risques de sécurité.

9.3.7 Coordination de la planification des interventions d'urgence

9.3.7.1 Par définition, une urgence est une situation ou un événement soudain, non planifié, exigeant une action immédiate. La coordination de la planification des interventions d'urgence désigne la planification d'activités qui ont lieu dans un laps de temps limité, pendant une situation d'urgence non planifiée, liée à l'exploitation aérienne. Un plan d'intervention en cas d'urgence (ERP) fait partie intégrante du processus de GRS des prestataires de services et vise à faire face à des urgences, crises ou événements aéronautiques. S'il existe une possibilité que l'exploitation aérienne ou les activités d'un prestataire de services soient compromises par des urgences telles qu'une urgence de santé publique/pandémie, ces scénarios devraient être abordés dans l'ERP de ce prestataire, selon les besoins. L'ERP devrait aborder les urgences prévisibles, telles qu'identifiées par le biais du SGS, et inclure des actions, processus et mesures d'atténuation visant à gérer efficacement les urgences aéronautiques.

9.3.7.2 L'objectif général de l'ERP est la poursuite sûre de l'exploitation et le retour le plus rapide possible aux opérations normales. L'ERP devrait garantir une transition ordonnée et efficace des opérations normales aux opérations d'urgence, y compris l'attribution de responsabilités et la délégation de pouvoirs en cas d'urgence. L'ERP inclut le laps de temps requis pour un retour aux opérations « normales » après l'urgence. L'ERP identifie les actions à entreprendre par le personnel responsable pendant une urgence. La plupart des urgences exigeront une action coordonnée entre différentes organisations, éventuellement avec d'autres prestataires de services et avec d'autres organisations externes, telles que des services d'urgence non liés à l'aviation. L'ERP devrait être facilement accessible au personnel approprié clé ainsi qu'aux organisations externes de coordination.

9.3.7.3 La coordination de la planification des interventions d'urgence ne s'applique qu'aux prestataires de services tenus d'établir et de tenir à jour un ERP. L'Annexe 19 n'exige pas la création ou l'élaboration d'un ERP ; la planification des interventions d'urgence est applicable uniquement à des prestataires de services spécifiques, comme indiqué dans les Annexes pertinentes de l'OACI (des termes différents pour les dispositions relatives au traitement des situations d'urgence peuvent être utilisés dans d'autres Annexes). Cette coordination devrait être exercée dans le cadre de tests périodiques de l'ERP.

9.3.8 Documentation relative au SGS

9.3.8.1 La documentation du SGS devrait inclure un « manuel du SGS » de haut niveau, qui décrit les politiques, processus et procédures du SGS du prestataire de services visant à faciliter l'administration interne, la communication et la tenue à jour du SGS de l'organisation. Elle devrait aider le personnel à comprendre comment fonctionne le SGS de l'organisation et comment la politique et les objectifs de sécurité seront réalisés. La documentation devrait inclure une description du système définissant les limites du SGS. Elle devrait aussi contribuer à clarifier la relation entre les politiques, processus, procédures et pratiques différents et définir la corrélation de ceux-ci avec la politique et les objectifs de sécurité du prestataire de services. La documentation devrait être adaptée aux activités quotidiennes de gestion de la sécurité et rédigée de manière à être facile à comprendre pour le personnel de l'ensemble de l'organisation.

9.3.8.2 Le manuel du SGS peut aussi servir d'outil de communication principal en matière de sécurité entre le prestataire de services et des parties prenantes clés en matière de sécurité (p. ex. l'AAC aux fins des processus réglementaires d'acceptation, d'évaluation et de suivi subséquent du SGS). Le manuel du SGS peut être un document indépendant ou il peut être intégré à d'autres documents (ou documentations) organisationnels tenus à jour par le prestataire de services. Si des détails des processus du SGS de l'organisation sont déjà exposés dans des documents existants, des références appropriées à ces documents suffisent. Ce document du SGS doit être tenu à jour. L'accord de l'AAC peut être requis avant que des amendements significatifs soient apportés au manuel du SGS, car il s'agit d'un manuel contrôlé.

9.3.8.3 Le manuel du SGS devrait inclure une description détaillée des politiques, processus et procédures du prestataire de services, notamment :

a) la politique et les objectifs de sécurité ;

b) des références à toute exigence réglementaire applicable au SGS ;

c) la description du système ;

d) les obligations de rendre compte en matière de sécurité et le personnel de sécurité clé ;

e) les processus et procédures du système de compte rendu volontaire et obligatoire en matière de sécurité ;

f) les processus et procédures d'identification des dangers et d'évaluation des risques de sécurité ;

g) les procédures d'enquête en matière de sécurité ;

h) les procédures d'établissement et de suivi des indicateurs de performance de sécurité ;

i) les processus et procédures de formation au SGS et la communication ;

j) les processus et procédures de communication en matière de sécurité ;

k) les procédures d'audit interne ;

l) les procédures de gestion du changement ;

m) les procédures de gestion de la documentation relative au SGS ;

n) le cas échéant, la coordination de la planification des interventions d'urgence.

9.3.8.4 La documentation du SGS inclut aussi la compilation et la tenue à jour des dossiers d'exploitation qui étayent l'existence et le fonctionnement permanent du SGS. Les dossiers d'exploitation sont les extrants des processus et procédures du SGS, tels que les activités de GRS et d'assurance de la sécurité. Les dossiers d'exploitation du SGS devraient être stockés et conservés conformément aux durées de conservation en vigueur. Les dossiers d'exploitation types du SGS devraient inclure :

a) les registres de dangers et les comptes rendus de dangers/sécurité ;

b) les SPI et diagrammes connexes ;

c) les dossiers des évaluations des risques de sécurité réalisées ;

d) les dossiers des examens ou audits internes réalisés dans le cadre du SGS ;

e) les dossiers d'audits internes ;

f) les dossiers de formation au SGS/à la sécurité ;

g) les procès-verbaux des réunions du comité du SGS/de la sécurité ;

h) le plan de mise en œuvre du SGS (pendant la mise en œuvre initiale) ;

i) l'analyse des lacunes à l'appui du plan de mise en œuvre.

9.4 COMPOSANT 2 : GESTION DES RISQUES DE SÉCURITÉ

9.4.1 Les prestataires de services devraient s'assurer qu'ils gèrent leurs risques de sécurité. Ce processus est appelé gestion des risques de sécurité (GRS) et inclut l'identification des dangers, l'évaluation des risques de sécurité et l'atténuation des risques de sécurité.

9.4.2 Le processus de GRS identifie systématiquement les dangers qui existent dans le contexte de la fourniture des produits ou services du prestataire. Les dangers peuvent résulter de systèmes présentant des déficiences au niveau de leur conception, de leur fonctionnement technique, de l'interface humains-systèmes ou des interactions de ces systèmes avec d'autres processus et systèmes. Ils peuvent aussi résulter d'une incapacité des processus ou systèmes existants à s'adapter à des changements dans l'environnement d'exploitation du prestataire de services. Une analyse minutieuse de ces facteurs peut souvent identifier des dangers potentiels en tout point du cycle de vie de l'exploitation ou de l'activité.

9.4.3 Il est essentiel de comprendre le système et son environnement d'exploitation pour réaliser une haute performance de sécurité. Une description détaillée du système définissant le système et ses interfaces aidera à acquérir cette compréhension. Des dangers peuvent être identifiés tout au long du cycle de vie opérationnelle depuis des sources internes et externes. Les évaluations des risques de sécurité et les mesures d'atténuation des risques de sécurité devront être sans cesse réexaminées afin de garantir le maintien de leur efficacité. La Figure 9-1 donne un aperçu général du processus d'identification des dangers et de gestion des risques de sécurité pour un prestataire de services.

Note.— Des orientations détaillées sur les procédures d'identification des dangers et d'évaluation des risques de sécurité sont données au Chapitre 2.

9.4.4 Identification des dangers

L'identification des dangers est la première étape du processus de GRS. Le prestataire de services devrait élaborer et tenir à jour un processus formel d'identification des dangers qui pourraient avoir une incidence sur la sécurité de l'aviation dans tous les domaines d'exploitation et activités. Ce processus inclut les équipements, installations et systèmes. Pour la sécurité de l'exploitation, il est important que tout danger lié à la sécurité de l'aviation soit identifié et maîtrisé. Il importe en outre d'envisager les dangers qui pourraient résulter d'interfaces du SGS avec des organisations externes.

Sources pour l'identification des dangers

9.4.4.1 Il existe une diversité de sources pour l'identification des dangers, tant à l'intérieur qu'à l'extérieur de l'organisation. Voici quelques exemples de sources internes :

a) *Suivi des opérations normales :* des techniques d'observation sont utilisées pour le suivi des opérations et activités quotidiennes, telles que les audits de sécurité en service de ligne (LOSA).

b) *Systèmes de suivi automatisés :* des systèmes d'enregistrement automatisés sont utilisés pour le suivi des paramètres qui peuvent être analysés ; c'est notamment le cas du suivi des données de vol (FDM).

c) *Systèmes de compte rendu volontaire et obligatoire en matière de sécurité :* ces systèmes offrent à tout le monde, y compris au personnel d'organisations externes, l'occasion de signaler des dangers et autres problèmes de sécurité à l'organisation.

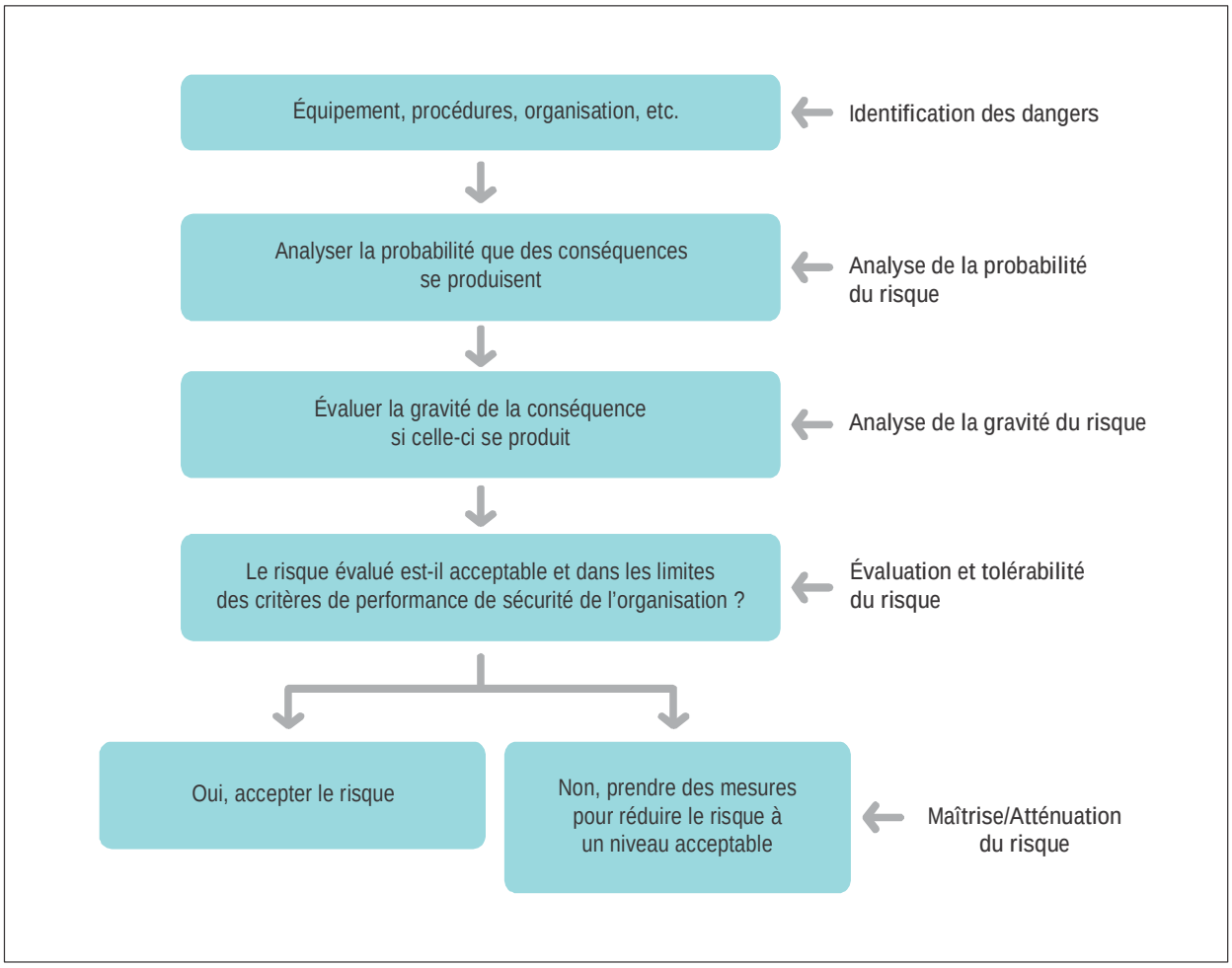

Figure 9-1. Processus d'identification des dangers et de gestion des risques

d) *Audits :* ceux-ci peuvent être utilisés pour identifier des dangers dans la tâche ou le processus soumis à audit. Ces audits devraient aussi être coordonnés avec des changements organisationnels afin d'identifier les dangers liés à la mise en œuvre du changement.

e) *Retours d'informations après formation :* une formation interactive (bidirectionnelle) peut faciliter l'identification de nouveaux dangers par les participants.

f) *Enquêtes en matière de sécurité menées par le prestataire de services :* les dangers identifiés au cours d'enquêtes de sécurité internes et les rapports de suivi sur les accidents/incidents.

9.4.4.2 Voici quelques exemples de sources externes pour l'identification des dangers :

a) *Comptes rendus d'accidents d'aviation :* examen des comptes rendus d'accidents ; il peut s'agir d'accidents survenus dans le même État ou à un type d'aéronef, dans une région ou un environnement d'exploitation similaires.

b) *Systèmes nationaux de compte rendu volontaire ou obligatoire en matière de sécurité :* certains États fournissent des résumés des comptes rendus de sécurité reçus d'autres prestataires de services.

c) *Audits de supervision réalisés par l'État ou par un tiers :* des audits externes peuvent parfois identifier des dangers. Ceux-ci peuvent être documentés en tant que dangers non identifiés ou perçus de manière moins évidente dans une constatation d'audit.

d) *Associations professionnelles et systèmes d'échange d'informations :* beaucoup d'associations professionnelles et de groupements d'industries sont en mesure de partager des données de sécurité pouvant inclure des dangers identifiés.

Système de compte rendu de sécurité

9.4.4.3 Une des principales sources d'identification des dangers est le système de compte rendu de sécurité, surtout le système de compte rendu volontaire en matière de sécurité. Alors que le système obligatoire est normalement utilisé pour des incidents qui se sont produits, le système volontaire offre un canal de compte rendu supplémentaire pour des problèmes de sécurité potentiels tels que des dangers, des quasi-collisions ou des erreurs. Ce type de compte rendu peut fournir des informations précieuses à l'État et au prestataire de services sur des événements aux conséquences mineures.

9.4.4.4 Il est important que les prestataires de services prévoient des protections appropriées pour encourager les gens à rendre compte de ce qu'ils voient ou vivent. Par exemple, une mesure coercitive peut être levée pour des comptes rendus d'erreurs ou, dans certaines circonstances, des violations des règles. Il devrait être clairement indiqué que les informations signalées seront utilisées exclusivement à l'appui de l'amélioration de la sécurité. Le but est de promouvoir une culture efficace du compte rendu et une mise en évidence proactive d'éventuelles carences en matière de sécurité.

9.4.4.5 Les systèmes de compte rendu volontaire en matière de sécurité devraient être confidentiels, ce qui implique que toute information identifiant l'auteur du compte rendu ne soit connue que du dépositaire, afin de permettre des actions de suivi. Le rôle du dépositaire devrait être limité à quelques individus, en général uniquement le gestionnaire de la sécurité et le personnel participant aux enquêtes en matière de sécurité. Le maintien de la confidentialité contribuera à faciliter la divulgation de dangers entraînant des erreurs humaines, sans crainte de sanctions ou d'embarras. Les comptes rendus volontaires en matière de sécurité peuvent être anonymisés et archivés une fois que les actions de suivi nécessaires ont été prises. Les comptes rendus anonymisés peuvent soutenir de futures analyses de tendances destinées à surveiller l'efficacité des mesures d'atténuation des risques et à identifier des dangers émergents.

9.4.4.6 Les membres du personnel à tous les niveaux, et toutes disciplines confondues, sont encouragés à identifier et signaler des dangers et autres problèmes de sécurité par l'intermédiaire de leurs systèmes de compte rendu en matière de sécurité. Pour être efficaces, les systèmes de compte rendu en matière de sécurité doivent être aisément accessibles à tous les membres du personnel. Selon la situation, un formulaire imprimé, en ligne ou sur ordinateur, peut être utilisé. La multiplicité des canaux de compte rendu maximise la probabilité que le personnel s'en serve. Tout le monde devrait être sensibilisé aux avantages qu'offrent les comptes rendus en matière de sécurité et devrait savoir que signaler.

9.4.4.7 Quiconque soumet un compte rendu en matière de sécurité devrait recevoir un retour d'informations sur les décisions ou les actions prises. L'harmonisation des exigences des systèmes de compte rendu, des outils d'analyse et des méthodes peut faciliter l'échange d'informations de sécurité ainsi que les comparaisons de certains indicateurs de performance de sécurité. Les retours d'informations aux auteurs des comptes rendus dans les systèmes de compte rendu volontaire servent aussi à montrer que de tels comptes rendus sont pris au sérieux. Cela contribue à promouvoir une culture positive de la sécurité et à encourager d'autres comptes rendus à l'avenir.

9.4.4.8 Il peut être nécessaire de filtrer les comptes rendus à l'entrée lorsqu'il y en a un grand nombre. Pour ce faire, il peut être utile de procéder à une évaluation initiale des risques de sécurité, afin de déterminer si une enquête plus approfondie s'impose et quel niveau d'enquête est requis.

9.4.4.9 Les comptes rendus en matière de sécurité sont souvent filtrés à l'aide d'une taxonomie ou d'un système de classification. Un filtrage des informations à l'aide d'une taxonomie peut faciliter l'identification de problèmes et tendances courants. Le prestataire de services devrait élaborer des taxonomies qui couvrent son ou ses types d'opérations. Le recours à une taxonomie présente l'inconvénient que le danger identifié ne correspond parfois pas clairement à l'une des catégories définies. Le défi est alors d'utiliser des taxonomies présentant le niveau de détail approprié, c'est-à-dire suffisamment spécifiques pour que les dangers soient faciles à attribuer à des catégories, mais suffisamment générales pour que les dangers soient utiles pour une analyse. Certains États et associations professionnelles internationales ont élaboré des taxonomies qui pourraient être utilisées. Le Chapitre 5 contient des informations supplémentaires sur les taxonomies.

9.4.4.10 D'autres méthodes d'identification des dangers incluent les ateliers ou les réunions dans lesquels des experts d'une matière spécifique présentent des scénarios d'analyse détaillés. Ces sessions tirent parti des contributions d'une vaste gamme de membres expérimentés du personnel technique et du personnel d'exploitation. Les réunions des comités de sécurité existants (SRB, SAG, etc.) pourraient être utilisées pour de telles activités ; le même groupe peut aussi être utilisé pour évaluer les risques de sécurité connexes.

9.4.4.11 Les dangers identifiés et leurs conséquences potentielles devraient être documentés. Cette documentation sera utilisée pour les processus d'évaluation des risques de sécurité.

9.4.4.12 Le processus d'identification des dangers envisage tous les dangers possibles pouvant exister dans le champ d'activités aéronautiques du prestataire de services, y compris aux interfaces avec d'autres systèmes, tant à l'intérieur qu'à l'extérieur de l'organisation. Une fois les dangers identifiés, leurs conséquences (à savoir tout événement ou résultat spécifique) devraient être déterminées.

Enquête sur les dangers

9.4.4.13 L'identification des dangers devrait être continue et faire partie intégrante des activités permanentes du prestataire de services. Certaines circonstances méritent parfois une enquête plus détaillée. Il peut s'agir, entre autres :

a) de cas où l'organisation connaît une augmentation inexpliquée d'événements liés à la sécurité de l'aviation ou de non-respect des réglementations ;

b) de modifications significatives de l'organisation ou de ses activités.

9.4.5 Enquête en matière de sécurité menée par le prestataire de services

9.4.5.1 Une gestion efficace de la sécurité dépend d'enquêtes de qualité, visant à analyser les événements de sécurité et les dangers pour la sécurité, et de constatations et recommandations de rapports, pour améliorer la sécurité dans l'environnement d'exploitation.

9.4.5.2 L'Annexe 13 établit une distinction claire entre enquêtes sur les accidents et incidents, d'une part, et enquêtes en matière de sécurité des prestataires de services, d'autre part. En vertu de l'Annexe 13, les enquêtes sur les accidents et les incidents graves relèvent de la responsabilité de l'État, telle que définie dans l'Annexe 13. Ce type d'informations est essentiel pour diffuser les leçons tirées des accidents et incidents. Les enquêtes en matière de sécurité des prestataires de services sont menées par les prestataires de services dans le cadre de leur SGS en vue de soutenir les processus d'identification des dangers et d'évaluation des risques. Beaucoup d'événements de sécurité ne relevant pas du champ d'application de l'Annexe 13 sont susceptibles de constituer une source précieuse d'informations pour l'identification de dangers ou de faiblesses dans les mesures de maîtrise des risques. Ces problèmes pourraient être mis au jour et résolus par une enquête en matière de sécurité menée par le prestataire de services.

9.4.5.3 L'objectif premier de l'enquête de sécurité du prestataire de services est de comprendre ce qui s'est produit et comment éviter que des situations similaires ne se produisent à l'avenir, en éliminant ou atténuant les carences en matière de sécurité. Un examen minutieux et méthodique de l'événement et l'application des leçons tirées permettent de réduire la probabilité et/ou les conséquences de répétitions de tels événements. Les enquêtes en matière de sécurité des prestataires de services font partie intégrante des SGS des prestataires de services.

9.4.5.4 Les enquêtes sur des événements de sécurité et des dangers pour la sécurité menées par les prestataires de services constituent une activité essentielle du processus général de gestion des risques en aviation. La réalisation d'une enquête en matière de sécurité offre notamment les avantages suivants :

a) permettre de mieux comprendre les événements ayant mené à cette occurrence ;

b) identifier les facteurs contributifs humains, techniques et organisationnels ;

c) identifier des dangers et réaliser des évaluations des risques ;

d) émettre des recommandations en vue de réduire ou d'éliminer les risques inacceptables ;

e) identifier les leçons tirées qui devraient être partagées avec les membres appropriés de la communauté aéronautique.

Facteurs déclencheurs d'enquêtes

9.4.5.5 Une enquête en matière de sécurité d'un prestataire de services est généralement déclenchée par une notification (rapport) soumise par le biais du système de compte rendu de sécurité. La Figure 9-2 présente les grandes lignes du processus décisionnel des enquêtes en matière de sécurité et la distinction entre les situations où une enquête en matière de sécurité d'un prestataire de services doit avoir lieu et les situations où une enquête doit être lancée en application des dispositions de l'Annexe 13.

9.4.5.6 Tous les événements ou dangers ne peuvent ni ne doivent faire l'objet d'enquêtes ; ce sont les conséquences réelles ou potentielles de l'événement ou du danger qui doivent déterminer s'il faut mener une enquête et quel doit en être le degré de détail. Les événements et dangers considérés comme pouvant présenter un haut risque sont plus susceptibles de faire l'objet d'enquêtes et devraient être analysés de façon plus approfondie que ceux qui ont un moindre potentiel de risque. Les prestataires de services devraient utiliser une approche décisionnelle structurée, avec des points de déclenchement prédéfinis. Ces points guideront les décisions dans l'enquête de sécurité, tant sur l'ampleur que sur la portée de l'enquête. Ces décisions pourraient comprendre les points suivants :

a) la gravité ou la gravité potentielle du résultat ;

b) les exigences réglementaires ou organisationnelles de mener une enquête ;

c) l'intérêt à en tirer pour la sécurité ;

d) l'occasion de prendre des mesures de sécurité ;

e) les risques associés à une absence d'enquête ;

f) la contribution à des programmes de sécurité ciblés ;

g) les tendances constatées ;

h) l'intérêt pour la formation ;

i) la disponibilité de ressources.

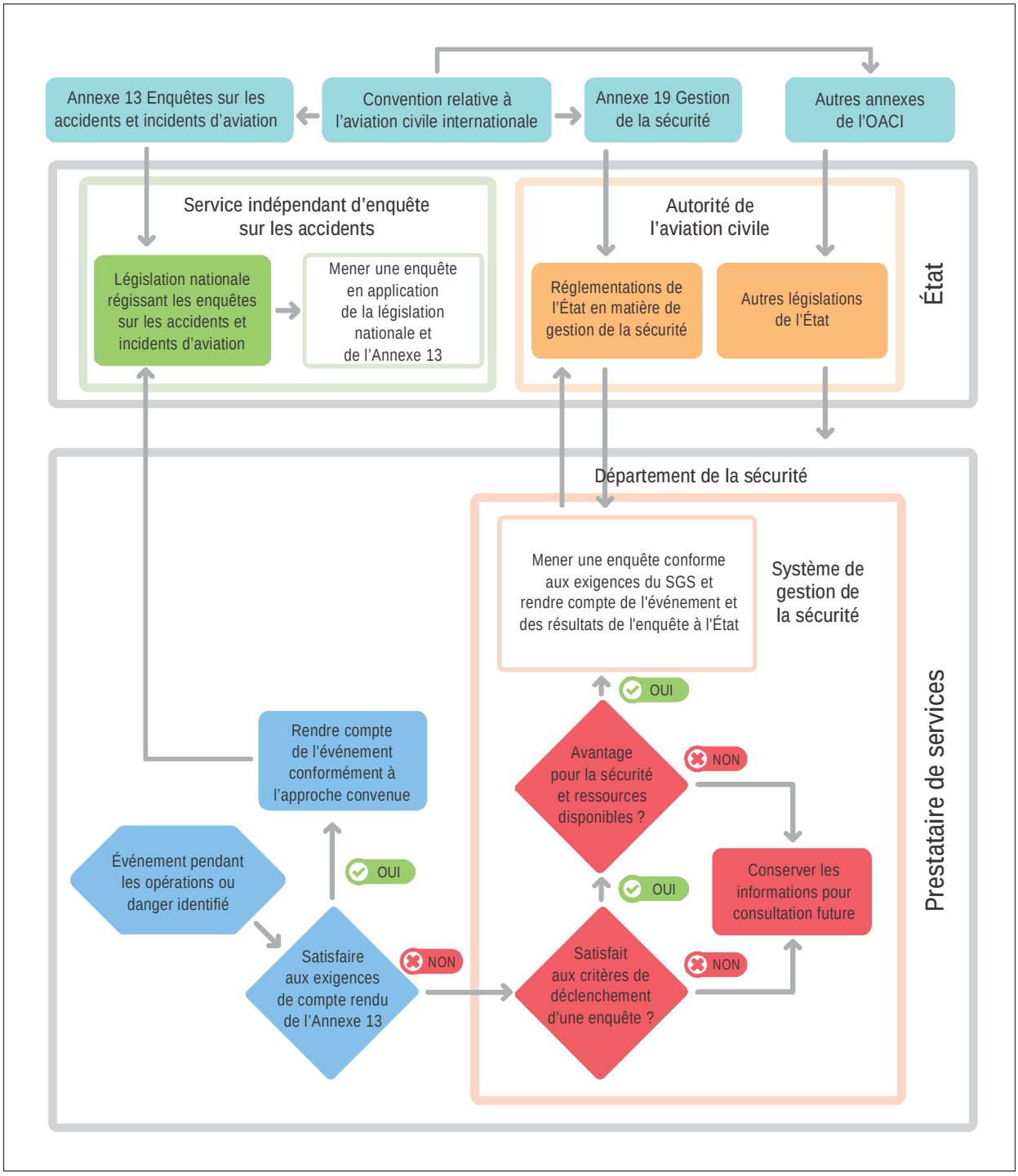

Figure 9-2. Processus décisionnel dans les enquêtes en matière de sécurité

Désignation d'un enquêteur

9.4.5.7 Si une enquête doit commencer, la première action sera de désigner un enquêteur ou, si les ressources sont disponibles, une équipe d'enquêteurs ayant les aptitudes et savoir-faire requis. La taille de l'équipe et le profil de spécialisation de ses membres dépendront de la nature et de la gravité de l'événement sur lequel doit porter l'enquête. L'équipe d'enquêteurs peut requérir l'aide d'autres spécialistes. Souvent, une seule personne est désignée pour une enquête interne et bénéficie de l'appui d'experts du service de l'exploitation et du service de la sécurité.

9.4.5.8 Les enquêteurs menant les enquêtes en matière de sécurité pour le prestataire de services sont idéalement indépendants d'un point de vue organisationnel du secteur associé à l'événement ou au danger identifié. On obtiendra de meilleurs résultats si le ou les enquêteurs connaissent le processus d'enquête de sécurité du prestataire de services (y ont été formés) et ont les aptitudes requises (l'expérience) pour mener de telles enquêtes. Les enquêteurs seront idéalement choisis pour ce rôle en raison de leurs connaissances, aptitudes et traits de caractère, qui incluent l'intégrité, l'objectivité, le raisonnement logique, le pragmatisme et l'approche indirecte.

Processus d'enquête

9.4.5.9 L'enquête devrait déterminer ce qui s'est produit et pourquoi, ce qui peut exiger l'application d'une analyse des causes premières dans le cadre de l'enquête. Idéalement, les personnes associées à l'événement devraient être interviewées dès que possible après cet événement. L'enquête devrait :

a) établir le déroulement des événements clés, y compris des actions des personnes associées à l'événement ;

b) analyser toutes les politiques et procédures liées à ces activités ;

c) analyser toute décision prise en relation avec cet événement ;

d) identifier toute mesure de maîtrise des risques mise en place qui aurait dû prévenir un tel événement ;

e) analyser les données de sécurité, à la recherche de tout événement précédent ou similaire.

9.4.5.10 L'enquête de sécurité devrait se concentrer sur les dangers et les risques de sécurité identifiés et sur les possibilités d'améliorations et non viser à blâmer ou à sanctionner. La façon dont l'enquête est menée et, surtout, la façon dont le rapport est rédigé influenceront l'incidence probable sur la sécurité, la future culture de la sécurité au sein de l'organisation et l'efficacité des futures initiatives en matière de sécurité.

9.4.5.11 L'enquête devrait conclure en exposant des constatations clairement définies et des recommandations qui éliminent ou atténuent les carences en matière de sécurité.

9.4.6 Évaluation et atténuation des risques de sécurité

9.4.6.1 Le prestataire de services doit élaborer un modèle et des procédures d'évaluation des risques de sécurité qui permettront l'application d'une approche cohérente et systématique pour l'évaluation des risques de sécurité. Un tel modèle devrait comporter une méthode pour déterminer quels risques de sécurité sont acceptables ou inacceptables et pour prioriser les actions.

9.4.6.2 Il faudra peut-être réexaminer et adapter régulièrement les outils de GRS utilisés, afin de garantir qu'ils soient appropriés à l'environnement d'exploitation du prestataire de services. Le prestataire de services peut trouver des approches plus sophistiquées qui reflètent mieux les besoins de son exploitation à mesure que son SGS atteint sa maturité. Le prestataire de services et l'AAC devraient convenir d'une méthodologie.

9.4.6.3 Des approches plus sophistiquées de la classification des risques de sécurité sont disponibles. Elles peuvent être plus appropriées si le prestataire de services est expérimenté en gestion de la sécurité ou s'il opère dans un environnement à haut risque.

9.4.6.4 Le processus d'évaluation des risques de sécurité devrait utiliser toutes les données de sécurité et informations de sécurité disponibles. Une fois que les risques de sécurité auront été évalués, le prestataire de services lancera un processus décisionnel fondé sur les données afin de déterminer quelles mesures de maîtrise des risques sont requises.

9.4.6.5 Les évaluations des risques de sécurité doivent parfois utiliser des informations qualitatives (jugement d'experts) plutôt que des données quantitatives en raison de la non-disponibilité de données. L'utilisation de la matrice des risques de sécurité permettra à l'utilisateur d'exprimer sous une forme chiffrée le ou les risques associés au danger identifié. Cela permet d'établir une comparaison directe d'ordre de grandeur entre risques de sécurité identifiés. Un critère d'évaluation qualitative des risques de sécurité tel que « se produira probablement » ou « improbable » peut être attribué à chaque risque de sécurité identifié, lorsque des données quantitatives ne sont pas disponibles.

9.4.6.6 Pour les prestataires de services qui ont des opérations en de multiples lieux avec des environnements d'exploitation spécifiques, il peut être plus efficace de créer des comités de sécurité locaux chargés de mener les évaluations des risques de sécurité et l'identification des mesures de maîtrise des risques de sécurité. Des conseils sont souvent demandés à un spécialiste du domaine d'exploitation (interne au prestataire de services ou externe). Dans certains cas, des autorités supérieures devront prendre des décisions finales ou accepter les mesures de maîtrise des risques pour que les ressources appropriées soient fournies.

9.4.6.7 Il appartient aux prestataires de services de décider de la façon dont ils priorisent leurs évaluations des risques de sécurité et adoptent des mesures de maîtrise des risques. À titre indicatif, le prestataire de services devrait trouver que le processus de priorisation :

a) évalue et maîtrise les risques de sécurité les plus élevés ;

b) affecte des ressources aux risques de sécurité les plus élevés ;

c) maintient ou améliore efficacement la sécurité ;

d) atteint les objectifs et SPT de sécurité déclarés et convenus ;

e) satisfait aux exigences des réglementations de l'État concernant la maîtrise des risques de sécurité.

9.4.6.8 Après l'évaluation des risques de sécurité, des mesures appropriées de maîtrise des risques peuvent être mises en œuvre. Il est important d'associer les « utilisateurs finals » et les experts du sujet à la détermination des mesures appropriées de maîtrise des risques de sécurité. En s'assurant que les personnes adéquates sont associées au processus, on maximise l'applicabilité des mesures d'atténuation des risques de sécurité choisies. Une détermination des conséquences involontaires, en particulier l'introduction de nouveaux dangers, devrait être réalisée avant la mise en œuvre de toute mesure de maîtrise des risques de sécurité.

9.4.6.9 Une fois que les mesures de maîtrise des risques de sécurité ont été convenues et mises en œuvre, il faudrait procéder au suivi de la performance de sécurité afin de s'assurer de l'efficacité des mesures de maîtrise des risques de sécurité. Cette étape est nécessaire pour vérifier l'intégrité, l'efficience et l'efficacité des nouvelles mesures de maîtrise des risques de sécurité en conditions d'exploitation.

9.4.6.10 Les extrants de la GRS devraient être documentés. Cette documentation devrait inclure le danger et toute conséquence de celui-ci, l'évaluation des risques de sécurité et toute mesure prise pour maîtriser les risques de sécurité. Ces informations sont souvent saisies dans un registre afin qu'un suivi et une surveillance puissent être pratiqués. Cette documentation de la GRS devient une source historique de connaissances en matière de sécurité organisationnelle qui

peut être utilisée comme référence pour la prise de décisions en matière de sécurité et pour l'échange d'informations de sécurité. Ces connaissances en matière de sécurité alimentent les analyses de tendances en matière de sécurité ainsi que les formations à la sécurité et la communication. Elles sont aussi utiles pour les audits internes pour permettre d'évaluer si les mesures et actions de maîtrise des risques de sécurité ont été mises en œuvre et sont efficaces.

9.5 COMPOSANT 3 : ASSURANCE DE LA SÉCURITÉ

9.5.1 L'Annexe 19, Appendice 2, § 3.1.1, exige que le prestataire de services élabore et tienne à jour les moyens permettant de vérifier la performance de l'organisation en matière de sécurité et de valider l'efficacité des mesures visant à maîtriser les risques de sécurité. Le composant « assurance de la sécurité » du SGS du prestataire de services fournit ces capacités.

9.5.2 L'assurance de la sécurité consiste en des processus et activités entrepris pour déterminer si le SGS fonctionne conformément aux attentes et aux exigences. À cette fin, elle suit en continu les processus ainsi que l'environnement d'exploitation pour détecter des changements ou des écarts qui pourraient introduire des risques de sécurité émergents ou entraîner une dégradation des mesures existantes de maîtrise des risques de sécurité. De tels changements ou écarts peuvent être traités au moyen du processus de GRS.

9.5.3 Les activités d'assurance de la sécurité devraient inclure l'élaboration et la mise en œuvre de mesures prises en réponse à tout problème identifié pouvant avoir une incidence sur la sécurité. Ces actions améliorent en permanence la performance du SGS du prestataire de services.

9.5.4 Suivi et mesure de la performance de sécurité

Pour vérifier la performance de sécurité et valider l'efficacité des mesures de maîtrise des risques de sécurité, il faut combiner les audits internes et la mise en place et le suivi de SPI. Il est important d'évaluer l'efficacité des mesures de maîtrise des risques de sécurité car leur application n'atteint pas toujours les résultats escomptés. L'évaluation permet d'identifier si la bonne mesure de maîtrise du risque a été sélectionnée et elle peut entraîner l'application d'une stratégie différente de maîtrise des risques de sécurité.

Audit interne

9.5.4.1 Des audits internes sont réalisés pour évaluer l'efficacité du SGS et pour identifier les domaines où des améliorations peuvent être apportées. La plupart des réglementations en matière de sécurité aérienne sont des mesures génériques de maîtrise des risques de sécurité établies par l'État. Assurer le respect de ces réglementations par le biais d'audits internes est un aspect essentiel de l'assurance de la sécurité.

9.5.4.2 Il est aussi nécessaire de s'assurer de l'efficacité de la mise en œuvre et du suivi de toute mesure de maîtrise des risques de sécurité. Les causes et facteurs contributifs devraient être étudiés et analysés si des non-conformités et d'autres problèmes sont décelés. L'audit interne se concentre surtout sur les politiques, processus et procédures qui régissent la prise de mesures de maîtrise des risques de sécurité.

9.5.4.3 Les audits internes sont le plus efficaces lorsqu'ils sont réalisés par des personnes ou des services indépendants des fonctions soumises à audit. Ces audits devraient donner au dirigeant responsable et à la haute direction des retours d'informations sur le degré :

a) de conformité aux réglementations ;

b) de conformité aux politiques, processus et procédures ;

c) d'efficacité des mesures de maîtrise des risques de sécurité ;

d) d'efficacité des mesures correctrices ;

e) d'efficacité du SGS.

9.5.4.4 Certaines organisations ne peuvent assurer une indépendance appropriée des audits internes. Dans ce cas, le prestataire de services devrait envisager d'engager des auditeurs externes (p. ex. des auditeurs indépendants ou des auditeurs d'une autre organisation).

9.5.4.5 La planification des audits internes devrait tenir compte de la criticité des processus pour la sécurité, des résultats d'audits et d'évaluations précédents (de toutes les sources), et des mesures de maîtrise des risques de sécurité mises en œuvre. Les audits internes devraient identifier des non-conformités aux réglementations et aux politiques, processus et procédures. Ils devraient aussi détecter des carences du système, un manque d'efficacité de mesures de maîtrise des risques de sécurité et des possibilités d'amélioration.

9.5.4.6 Il est essentiel d'évaluer tant la conformité que l'efficacité pour réaliser une bonne performance de sécurité. Le processus d'audit interne peut être utilisé pour déterminer tant la conformité que l'efficacité. Les questions suivantes peuvent être posées pour évaluer la conformité et l'efficacité de chaque processus ou procédure :

a) Pour déterminer la conformité

1) La procédure ou le processus requis existe-t-il ?

2) La procédure ou le processus est-il documenté (intrants, activités, interfaces et extrants définis) ?

3) La procédure ou le processus répond-il aux exigences (critères) ?

4) La procédure ou le processus est-il utilisé ?

5) Tous les membres du personnel concernés suivent-ils en permanence le processus ou la procédure ?

6) Les extrants définis sont-ils en cours de production ?

7) Un changement de processus ou de procédure a-t-il été documenté et mis en œuvre ?

b) Pour évaluer l'efficacité

1) Les utilisateurs comprennent-ils le processus ou la procédure ?

2) Le but du processus ou de la procédure est-il systématiquement atteint ?

3) Les résultats du processus ou de la procédure correspondent-ils aux attentes du « client » ?

4) La procédure ou le processus est-il révisé régulièrement ?

5) Une évaluation des risques de sécurité est-elle menée en cas de modifications du processus ou de la procédure ?

6) Des améliorations apportées au processus ou à la procédure ont-elles généré les avantages escomptés ?

9.5.4.7 De plus, les audits internes devraient suivre les progrès engrangés sur la voie de la résolution des non-conformités identifiées précédemment. Celles-ci doivent avoir été gérées par une analyse des causes premières et par l'élaboration et la mise en œuvre de plans d'actions correctrices et préventives. Les résultats de l'analyse de la ou des causes et facteurs contributifs de toute non-conformité devraient alimenter les processus de GRS du prestataire de services.

9.5.4.8 Les résultats du processus d'audit interne deviennent un des divers intrants des fonctions de GRS et d'assurance de la sécurité. Les audits internes informent la direction du prestataire de services quant au niveau de conformité au sein de l'organisation, au degré d'efficacité des mesures de maîtrise des risques de sécurité et aux domaines nécessitant la prise de mesures correctrices ou préventives.

9.5.4.9 Les AAC peuvent fournir des rétro-informations supplémentaires sur l'état de conformité aux réglementations et sur l'efficacité du SGS, des associations professionnelles ou d'autres tiers sélectionnés par le prestataire de services pour procéder à l'audit de son organisation et de ses processus. Les résultats de tels audits de seconde ou de tierce partie alimentent la fonction d'assurance de la sécurité et fournissent au prestataire de services des indications sur l'efficacité de ses processus d'audit interne ainsi que des possibilités d'améliorer son SGS.

Suivi de la performance de sécurité

9.5.4.10 Le suivi de la performance de sécurité se fait par la collecte de données de sécurité et d'informations de sécurité auprès d'une diversité de sources généralement à la disposition d'une organisation. La disponibilité de données à l'appui d'un processus décisionnel éclairé est un des aspects les plus importants du SGS. L'utilisation de ces données pour suivre et mesurer la performance de sécurité est une activité essentielle qui génère les informations requises pour prendre des décisions concernant les risques de sécurité.

9.5.4.11 Le suivi et la mesure de la performance de sécurité devraient être réalisés conformément à quelques principes de base. La performance de sécurité atteinte donne une indication quant au comportement organisationnel et constitue aussi une mesure de l'efficacité du SGS. À cet égard, l'organisation doit définir :

a) des objectifs de sécurité, qui devraient être fixés d'abord pour refléter les réalisations stratégiques ou les résultats souhaités en rapport avec des préoccupations de sécurité spécifiques au contexte d'exploitation de l'organisation ;

b) des SPI, qui sont des paramètres tactiques liés aux objectifs de sécurité et constituent dès lors la référence pour la collecte des données ;

c) des SPT, qui sont aussi des paramètres tactiques utilisés pour assurer le suivi des progrès sur la voie de la réalisation des objectifs de sécurité.

9.5.4.12 Un bilan plus complet et réaliste de la performance de sécurité du prestataire de services sera obtenu si les SPI couvrent un large spectre d'indicateurs. Ces indicateurs devraient inclure :

a) les événements à faible probabilité/haute gravité (p. ex. accidents et incidents graves) ;

b) les événements à haute probabilité/faible gravité (p. ex. des événements opérationnels sans conséquences, des rapports de non-conformité, des écarts, etc.) ;

c) la performance des processus (p. ex. formation, améliorations des systèmes et traitement des rapports).

9.5.4.13 Les SPI sont utilisés pour mesurer la performance de sécurité opérationnelle du prestataire de services et la performance de son SGS. Les SPI reposent sur le suivi des données et des informations obtenues de diverses

sources, y compris du système de compte rendu en matière de sécurité. Ils devraient être spécifiques au prestataire de services concerné et être liés aux objectifs de sécurité déjà établis.

9.5.4.14 Lorsqu'ils établissent leurs SPI, les prestataires de services devraient tenir compte des points suivants :

a) *Mesurer les paramètres corrects :* Il faut déterminer les meilleurs SPI qui montreront que l'organisation est en bonne voie d'atteindre ses objectifs de sécurité. Il faut aussi s'interroger sur les plus gros problèmes de sécurité et risques de sécurité auxquels l'organisation est confrontée et identifier les SPI qui pourront révéler la maîtrise efficace de ces risques.

b) *Disponibilité des données :* Existe-t-il des données disponibles qui correspondent à ce que l'organisation veut mesurer ? Dans la négative, il peut être nécessaire d'établir des sources supplémentaires de collecte de données. Pour les petites organisations disposant de quantités limitées de données, la mise en commun d'ensembles de données peut aussi aider à identifier des tendances. À cet égard, un appui peut être obtenu auprès d'associations professionnelles qui peuvent collationner des données de sécurité de multiples organisations.

c) *Fiabilité des données :* Les données peuvent manquer de fiabilité parce qu'elles sont subjectives ou incomplètes.

d) *SPI communs au secteur d'activités :* Il peut être utile de convenir de SPI communs avec des organisations similaires afin de permettre des comparaisons entre organisations. L'autorité de réglementation ou les associations professionnelles pourraient faciliter cela.

9.5.4.15 Une fois que les SPI ont été établis, le prestataire de services devrait s'interroger sur l'opportunité de déterminer des SPT et des niveaux d'alerte. Les SPT sont utiles pour encourager des améliorations de la sécurité, mais il s'est avéré que, mal mises en œuvre, elles peuvent favoriser des comportements non souhaitables plutôt qu'une amélioration de la performance de sécurité organisationnelle. En effet, si des individus et des services deviennent trop attachés à atteindre la cible, ils perdent parfois de vue les raisons ayant présidé à l'établissement de cette cible. Dans ces cas, il peut être plus approprié de réaliser un suivi du SPI pour déceler des tendances.

9.5.4.16 Les activités suivantes peuvent fournir des sources pour le suivi et la mesure de la performance de sécurité :

a) *Les études de sécurité* sont des analyses destinées à offrir une compréhension plus approfondie des problèmes de sécurité ou d'une tendance de la performance de sécurité.

b) *L'analyse des données de sécurité* utilise les données des comptes rendus en matière de sécurité pour mettre au jour des problèmes ou tendances courants susceptibles de mériter une enquête plus approfondie.

c) *Les enquêtes en matière de sécurité* examinent les procédures ou processus liés à une opération spécifique. Elles peuvent recourir à des listes de vérification, des questionnaires et des entretiens confidentiels informels. Les enquêtes en matière de sécurité fournissent généralement des informations qualitatives. Il faudra parfois procéder à une validation s'appuyant sur une collecte de données afin de déterminer si des mesures correctrices sont requises. Néanmoins, ces enquêtes peuvent fournir une source précieuse et peu onéreuse d'informations de sécurité.

d) *Les audits de sécurité* s'attachent à évaluer l'intégrité du SGS et des systèmes d'appui du prestataire de services. Les audits de sécurité peuvent aussi servir à évaluer l'efficacité des mesures de maîtrise des risques de sécurité mises en place ou à assurer le suivi de la conformité aux réglementations en matière de sécurité. Assurer l'indépendance et l'objectivité est un défi pour les audits de sécurité. Il est possible d'assurer indépendance et objectivité en engageant des entités externes ou en menant des

audits internes après avoir mis en place des protections (politiques, procédures, rôles, protocoles de communication).

e) *Les constatations et recommandations d'enquêtes en matière de sécurité* peuvent fournir des informations de sécurité utiles qui peuvent être analysées par rapport à d'autres données de sécurité collectées.

f) *Les systèmes de collecte des données opérationnelles* tels que FDA et informations radar peuvent fournir des données utiles sur des événements et sur la performance opérationnelle.

9.5.4.17 L'élaboration de SPI devrait être liée aux objectifs de sécurité et basée sur l'analyse de données qui sont disponibles et accessibles. Le processus de suivi et de mesure requiert l'utilisation d'indicateurs de performance de sécurité sélectionnés, de SPT correspondantes et de facteurs déclencheurs en matière de sécurité.

9.5.4.18 L'organisation devrait assurer le suivi de la performance des SPI et SPT établis pour identifier des changements anormaux dans la performance de sécurité. Les SPT devraient être réalistes, spécifiques au contexte et réalisables compte tenu des ressources à la disposition de l'organisation et du secteur aéronautique connexe.

9.5.4.19 Essentiellement, le suivi et la mesure de la performance de sécurité fournissent un moyen de vérifier l'efficacité des mesures de maîtrise des risques de sécurité. De plus, ils permettent de mesurer l'intégrité et l'efficacité des processus et activités du SGS.

9.5.4.20 L'État peut avoir des processus spécifiques pour l'acceptation des SPI et des SPT, processus qui devront être suivis. Par conséquent, pendant l'élaboration de SPI et de SPT, le prestataire de services devrait consulter l'autorité de réglementation dont dépend l'organisation ou consulter toute information connexe publiée par l'État.

9.5.4.21 Pour de plus amples informations sur la gestion de la performance de sécurité, voir le Chapitre 4.

9.5.5 La gestion du changement

9.5.5.1 Les prestataires de services connaissent des changements dus à plusieurs facteurs, notamment, mais sans s'y limiter :

a) une expansion ou une contraction de l'organisation ;

b) des améliorations apportées à l'entreprise qui ont une incidence sur la sécurité ; elles peuvent entraîner des modifications de systèmes, processus ou procédures internes qui soutiennent la fourniture sûre de produits et services ;

c) des modifications de l'environnement d'exploitation de l'organisation ;

d) des modifications aux interfaces du SGS avec des organisations externes ;

e) des changements des réglementations externes, des changements économiques et des risques émergents.

9.5.5.2 Les changements peuvent avoir une incidence sur l'efficacité des mesures existantes de maîtrise des risques de sécurité. De plus, de nouveaux dangers et les risques de sécurité qui y sont associés peuvent être introduits par inadvertance dans une opération lorsqu'un changement se produit. Les dangers devraient être identifiés et les risques de sécurité connexes devraient être évalués et maîtrisés comme indiqué dans les procédures existantes d'identification des dangers ou dans les procédures de GRS de l'organisation.

9.5.5.3 Le processus de l'organisation pour la gestion du changement devrait tenir compte des points suivants :

a) Criticité. Dans quelle mesure le changement est-il critique ? Le prestataire de services devrait envisager l'incidence sur les activités de son organisation et l'incidence sur d'autres organisations et sur le système aéronautique.

b) Disponibilité d'experts du sujet. Il est important que des membres clés de la communauté aéronautique soient associés aux activités de gestion du changement, éventuellement des individus provenant d'organisations externes.

c) Disponibilité de données et informations sur la performance de sécurité. Quelles données et informations disponibles peuvent être utilisées pour donner des informations sur la situation et permettre une analyse du changement ?

9.5.5.4 De petits changements progressifs passent souvent inaperçus mais l'effet cumulatif peut être considérable. Des changements, qu'ils soient majeurs ou mineurs, peuvent affecter la description du système de l'organisation et peuvent rendre une révision nécessaire. C'est pourquoi la description du système devrait être réexaminée régulièrement pour déterminer si elle reste valable, étant donné que la plupart des prestataires de services connaissent des changements réguliers, voire continus.

9.5.5.5 Le prestataire de services devrait définir le facteur déclencheur du processus de gestion formelle de changement. Les changements susceptibles de déclencher une gestion formelle du changement comprennent :

a) l'introduction de technologies ou équipements nouveaux ;

b) des modifications de l'environnement d'exploitation ;

c) des changements dans le personnel clé ;

d) des changements significatifs des niveaux de dotation en personnel ;

e) des changements dans les exigences réglementaires relatives à la sécurité ;

f) une importante restructuration de l'organisation ;

g) des changements physiques (nouvelle installation ou base, modifications du plan général de l'aérodrome, etc.).

9.5.5.6 Le prestataire de services devrait aussi tenir compte de l'incidence du changement sur le personnel. Celle-ci pourrait influer sur la façon dont le changement est accepté par les personnes concernées. Une communication et un engagement précoces amélioreront normalement la façon dont le changement est perçu et mis en œuvre.

9.5.5.7 Le processus de gestion du changement devrait inclure les activités suivantes :

a) *comprendre et définir le changement :* il faudrait fournir une description du changement et expliquer pourquoi ce changement est mis en œuvre ;

b) *comprendre et définir sur qui et sur quoi ce changement aura une incidence :* il peut s'agir d'individus au sein de l'organisation, d'autres services ou de personnes ou organisations extérieures. Des équipements, systèmes et processus peuvent aussi être touchés. Un examen de la description du système et des interfaces des organisations peut s'avérer nécessaire. Il s'agit-là d'une occasion d'établir qui devrait être associé au changement. Des changements peuvent avoir des incidences sur des mesures de maîtrise des risques déjà en place pour atténuer d'autres risques et, par conséquent,

le changement pourrait augmenter les risques dans des domaines qui ne sautent pas immédiatement aux yeux ;

c) *identifier les dangers liés au changement et procéder à une évaluation des risques de sécurité :* il s'agit ici d'identifier tout danger directement lié au changement. L'incidence sur les dangers existants et sur les mesures de maîtrise des risques de sécurité pouvant être affectées par le changement devrait aussi être analysée. Cette étape devrait utiliser les processus existants de GRS de l'organisation ;

d) *élaborer un plan d'action :* celui-ci devrait définir ce qu'il faut faire, qui doit le faire et pour quand. Il devrait y avoir un plan clair décrivant comment le changement sera mis en œuvre et qui sera responsable de quelles actions, ainsi que la séquence et le calendrier de chaque tâche ;

e) *accord pour ce changement :* il vise à confirmer que le changement peut être mis en œuvre en toute sécurité. La personne qui assume la responsabilité générale du changement et est habilitée à le mettre en œuvre devrait signer le plan de changement pour accord ;

f) *plan d'assurance :* il vise à déterminer quelles actions de suivi sont requises. Il faut étudier comment le changement sera communiqué et si des activités supplémentaires (telles que des audits) sont nécessaires pendant ou après le changement. Toute hypothèse formulée doit être testée.

9.5.6 Amélioration continue du SGS

9.5.6.1 L'Annexe 19, Appendice 2, § 3.3, exige : « Le prestataire de services suivra et évaluera l'efficacité des processus de son SGS afin de maintenir ou de constamment améliorer l'efficacité globale du SGS. » Le maintien et l'amélioration continue de l'efficacité du SGS du prestataire de services sont soutenus par des activités d'assurance de la sécurité incluant la vérification et le suivi d'actions et de processus d'audit internes. Il convient de reconnaître que le maintien et l'amélioration continue du SGS constituent une quête perpétuelle car l'organisation elle-même et l'environnement d'exploitation seront en constante évolution.

9.5.6.2 Les audits internes impliquent l'évaluation des activités aéronautiques du prestataire de services qui peuvent fournir des informations utiles pour les processus décisionnels de l'organisation. La fonction d'audit interne inclut l'évaluation de toutes les fonctions de gestion de la sécurité dans l'ensemble de l'organisation.

9.5.6.3 L'efficacité du SGS ne devrait pas reposer uniquement sur les SPI ; les prestataires de services devraient viser à mettre en œuvre toute une diversité de méthodes pour déterminer son efficacité, mesurer les extrants ainsi que les résultats des processus et évaluer les informations collectées par le biais de ces activités. Ces méthodes peuvent comprendre :

a) *des audits :* sont compris dans cette catégorie, les audits internes et les audits menés par d'autres organisations ;

b) *des évaluations :* cette catégorie inclut les évaluations de la culture de la sécurité et de l'efficacité du SGS ;

c) *le suivi des événements :* le suivi de la récurrence d'événements de sécurité, y compris des accidents et incidents ainsi que des erreurs et des situations de violation des règles ;

d) *des enquêtes en matière de sécurité :* cette catégorie comprend les enquêtes sur la culture qui livrent des rétro-informations utiles sur l'engagement du personnel à appliquer le SGS. Ces enquêtes peuvent aussi fournir un indicateur de la culture de la sécurité au sein de l'organisation ;

e) *des examens de la gestion :* il s'agit ici d'examiner si l'organisation est en voie d'atteindre ses objectifs de sécurité et d'avoir une occasion d'analyser toutes les informations disponibles sur la performance de sécurité afin de dégager des tendances générales. Il est important que la haute direction examine l'efficacité du SGS. Ce travail peut être inclus dans les fonctions du comité de sécurité de haut niveau ;

f) *l'évaluation des SPI et des SPT :* éventuellement dans le cadre de l'examen de la gestion. Cette évaluation étudie les tendances et, si des données appropriées sont disponibles, elle peut être comparée à celle d'autres prestataires de services ou de l'État ou avec des données mondiales ;

g) *les leçons tirées* des systèmes de compte rendu en matière de sécurité et des enquêtes en matière de sécurité réalisées par des prestataires de services. Elles devraient mener à la mise en œuvre d'améliorations de la sécurité.

9.5.6.4 En résumé, le suivi de la performance de sécurité et des processus d'audit interne contribue à soutenir la capacité du prestataire de services à constamment améliorer sa performance de sécurité. Le suivi permanent du SGS, des mesures connexes de maîtrise des risques de sécurité et des systèmes d'appui garantit au prestataire de services et à l'État que les processus de gestion de la sécurité atteignent leurs objectifs souhaités en matière de performance de sécurité.

9.6 COMPOSANT 4 : PROMOTION DE LA SÉCURITÉ

9.6.1 La promotion de la sécurité encourage une culture positive de la sécurité et contribue à réaliser les objectifs de sécurité du prestataire de services par le biais de la combinaison de compétences techniques sans cesse renforcées par la formation, la sensibilisation, une communication efficace et le partage d'informations. La haute direction joue un rôle de chef de file dans la promotion d'une culture de la sécurité dans toute l'organisation.

9.6.2 Il est impossible d'assurer une gestion efficace de la sécurité uniquement par mandat ou par respect strict des politiques et procédures. La promotion de la sécurité vise les comportements tant individuels qu'organisationnels et complète les politiques, procédures et processus de l'organisation en fournissant un système de valeurs à l'appui des efforts en matière de sécurité.

9.6.3 Le prestataire de services doit établir et mettre en œuvre des processus et procédures qui facilitent une communication bidirectionnelle efficace à tous les échelons de l'organisation. Il devrait notamment donner une direction stratégique claire depuis le sommet de l'organisation et permettre une communication ascendante qui encourage tous les membres du personnel à donner des rétro-informations franches et constructives.

9.6.4 Formation et sensibilisation

9.6.4.1 L'Annexe 19 exige : « Le prestataire de services élaborera et tiendra à jour un programme de formation en matière de sécurité qui garantit que le personnel sera formé et compétent pour exécuter les tâches liées au SGS. » Elle stipule en outre : « La portée du programme de formation en matière de sécurité correspondra à la participation de chaque stagiaire au SGS. » Le gestionnaire de la sécurité est chargé de garantir qu'un programme de formation approprié est mis en place. Un tel programme doit notamment fournir des informations appropriées en matière de sécurité qui soient pertinentes au vu des problèmes de sécurité spécifiques rencontrés par l'organisation. Le fait que les membres du personnel soient formés et compétents pour exécuter leurs tâches liées au SGS, indépendamment de leur place dans l'organigramme de l'organisation, est un gage de l'engagement de la direction en faveur d'un SGS efficace. Le programme de formation devrait inclure des exigences de formation initiale et périodique pour maintenir les compétences à jour. La formation initiale à la sécurité devrait porter, au minimum, sur les points suivants :

a) les politiques et objectifs de sécurité de l'organisation ;

b) les rôles et responsabilités liés à la sécurité au sein de l'organisation ;

c) les principes de base de la GRS ;

d) les systèmes de compte rendu de sécurité ;

e) les processus et procédures du SGS de l'organisation ;

f) les facteurs humains.

9.6.4.2 La formation périodique à la sécurité devrait se concentrer sur les modifications apportées aux politiques, processus et procédures du SGS et devrait mettre en lumière tout problème de sécurité spécifique pertinent pour l'organisation ou les leçons tirées.

9.6.4.3 Le programme de formation devrait être adapté aux besoins inhérents au rôle de la personne dans le SGS. Par exemple, la formation des cadres participant aux comités de sécurité de l'organisation sera d'un niveau et d'une portée dépassant la formation destinée aux membres du personnel participant directement à la fourniture des produits ou services de l'organisation. Les membres du personnel ne participant pas directement à l'exploitation auront peut-être besoin uniquement d'un aperçu de haut niveau du SGS de l'organisation.

Analyse des besoins de formation

9.6.4.4 Pour la plupart des organisations, il est nécessaire de procéder à une analyse formelle des besoins de formation (TNA) pour s'assurer qu'il existe une compréhension claire de l'exploitation, des tâches du personnel liées à la sécurité et de la formation disponible. Une TNA type commence normalement par la réalisation d'une analyse du public cible, qui inclut généralement les étapes suivantes :

a) Chaque membre du personnel du prestataire de services sera affecté par la mise en œuvre du SGS mais pas de la même manière ni au même degré. Il faut identifier chaque groupe de membres du personnel et déterminer leur interaction avec les processus de gestion de la sécurité, les intrants et les extrants, en particulier avec les tâches liées à la sécurité. Ces informations devraient être disponibles dans les descriptions de poste/rôle. Normalement elles commenceront à faire apparaître des groupements d'individus ayant des besoins d'apprentissage similaires. Le prestataire de services devrait étudier s'il est judicieux d'étendre l'analyse au personnel en interface avec des organisations externes.

b) Il faut identifier les connaissances et compétences requises pour effectuer chaque tâche liée à la sécurité et requises pour chaque groupe de membres du personnel.

c) Il faut mener une analyse en vue d'identifier les lacunes entre les aptitudes et connaissances actuelles en matière de sécurité parmi le personnel et les aptitudes et compétences requises pour exécuter efficacement les tâches attribuées en matière de sécurité.

d) Il faut identifier l'approche du développement des aptitudes et connaissances la plus appropriée pour chaque groupe en vue d'élaborer un programme de formation adapté au rôle de chaque individu ou groupe dans la gestion de la sécurité. Le programme de formation devrait aussi tenir compte des besoins permanents de connaissances et de compétences du personnel en matière de sécurité ; ces besoins seront généralement satisfaits grâce à un programme de formation périodique.

9.6.4.5 Il est aussi important d'identifier la méthode appropriée pour donner cette formation. L'objectif principal est qu'au terme de la formation, le personnel ait les compétences requises pour exécuter ses tâches liées au SGS. Le critère généralement le plus important est la compétence des formateurs ; leur engagement, leurs aptitudes

pédagogiques et leur maîtrise de la gestion de la sécurité auront une incidence significative sur l'efficacité de la formation donnée. Le programme de formation à la sécurité devrait aussi spécifier les responsabilités liées à l'élaboration de contenus et de calendriers de formation ainsi que la gestion des dossiers de formation et de compétences.

9.6.4.6 L'organisation devrait déterminer qui doit être formé et à quel niveau, et cette décision dépendra de la participation de chacun au SGS. La plupart des travailleurs de l'organisation ont un lien direct ou indirect avec la sécurité de l'aviation et, donc, des tâches liées au SGS. C'est le cas de tout membre du personnel associé directement à la fourniture de produits et services et du personnel participant aux comités de sécurité de l'organisation. Certains membres du personnel administratif et d'appui auront un rôle limité dans le SGS mais auront besoin d'une formation au SGS car leur travail peut malgré tout avoir une incidence indirecte sur la sécurité de l'aviation.

9.6.4.7 Le prestataire de services devrait identifier les tâches du personnel liées au SGS et utiliser ces informations pour examiner le programme de formation à la sécurité et veiller à ce que chaque individu reçoive une formation adaptée à son rôle dans le SGS. Le programme de formation à la sécurité devrait préciser le contenu de la formation à la sécurité pour le personnel d'appui, le personnel d'exploitation, les directeurs et superviseurs, les cadres supérieurs et le dirigeant responsable.

9.6.4.8 Le dirigeant responsable et les cadres supérieurs devraient suivre une formation spécifique à la sécurité couvrant les sujets suivants :

a) une formation de sensibilisation spécifique pour les nouveaux dirigeants responsables et titulaires de postes concernant leurs obligations de rendre compte et leurs responsabilités dans le cadre du SGS ;

b) l'importance de respecter les exigences de sécurité nationales et organisationnelles ;

c) l'engagement de la direction ;

d) l'affectation des ressources ;

e) la promotion de la politique de sécurité et du SGS ;

f) la promotion d'une culture positive de la sécurité ;

g) une communication efficace entre les services pour ce qui est de la sécurité ;

h) l'objectif de sécurité, les SPT et les niveaux d'alerte ;

i) la politique disciplinaire.

9.6.4.9 Le principal but du programme de formation à la sécurité est de garantir que le personnel, à tous les échelons de l'organisation, maintient à jour ses compétences pour assumer ses rôles en matière de sécurité ; par conséquent, les compétences du personnel devraient être réexaminées régulièrement.

9.6.5 Communication en matière de sécurité

9.6.5.1 Le prestataire de services doit communiquer les objectifs et procédures du SGS de l'organisation à tout le personnel concerné. Il devrait mettre en place une stratégie de communication qui permet la diffusion des communications en matière de sécurité par la méthode la plus appropriée, sur la base du rôle de chaque individu et du besoin de chaque individu de recevoir des informations liées à la sécurité. À cette fin, des lettres d'information, avis, bulletins, briefings ou formations en matière de sécurité peuvent être utilisés. Le gestionnaire de la sécurité devrait aussi s'assurer que les leçons tirées d'enquêtes et d'antécédents ou d'expériences, tant internes que d'autres organisations, soient largement diffusées. La communication en matière de sécurité vise donc à :

a) *veiller à ce que le personnel soit bien au courant du SGS :* c'est une bonne manière de promouvoir la politique et les objectifs de sécurité de l'organisation ;

b) *transmettre des informations cruciales pour la sécurité :* des informations cruciales pour la sécurité sont des informations spécifiques relatives à des problèmes de sécurité et à des risques de sécurité qui sont susceptibles d'exposer l'organisation à un risque de sécurité. Elles pourraient provenir d'informations de sécurité collectées à partir de sources internes ou externes, telles que des leçons tirées, ou être liées à des mesures de maîtrise des risques de sécurité. Le prestataire de services détermine quelles informations sont considérées comme cruciales pour la sécurité et à quel moment il convient de les communiquer ;

c) *mieux sensibiliser aux nouvelles mesures de maîtrise des risques de sécurité et aux mesures correctrices :* les risques de sécurité auxquels le prestataire de services est confronté évolueront au fil du temps et qu'il s'agisse d'un nouveau risque de sécurité identifié ou de modifications apportées à des mesures de maîtrise des risques de sécurité, ces changements devront être communiqués au personnel concerné ;

d) *fournir des informations sur les procédures de sécurité nouvelles ou amendées :* lors de l'actualisation des procédures de sécurité, il est important que les personnes appropriées soient mises au courant des changements ;

e) *promouvoir une culture positive de la sécurité et à encourager le personnel à identifier des dangers et à en rendre compte :* la communication en matière de sécurité est bidirectionnelle. Il est important que tout le personnel communique des problèmes de sécurité à l'organisation par l'intermédiaire du système de compte rendu en matière de sécurité ;

f) *fournir des rétro-informations* au personnel qui soumet des comptes rendus en matière de sécurité quant aux mesures qui ont été prises pour répondre à toute préoccupation identifiée.

9.6.5.2 Les prestataires de services devraient examiner si l'une quelconque des informations de sécurité énumérées ci-dessus doit être communiquée à des organisations externes.

9.6.5.3 Les prestataires de services devraient évaluer l'efficacité de leur communication en matière de sécurité en vérifiant que le personnel a reçu et a compris toute information cruciale pour la sécurité qui a été diffusée. Ils peuvent le faire dans le cadre d'activités d'audit interne ou de l'évaluation de l'efficacité du SGS.

9.6.5.4 Des activités de promotion de la sécurité devraient être menées tout au long du cycle de vie du SGS, pas uniquement au début de sa mise en œuvre.

9.7 PLANIFICATION DE LA MISE EN ŒUVRE

9.7.1 Description du système

9.7.1.1 Une description du système contribue à répertorier les processus organisationnels, y compris toute interface, et à définir la portée du SGS. Elle offre une occasion de recenser des lacunes liées aux composants et éléments du SGS du prestataire de services et peut servir de point de départ pour identifier des dangers organisationnels ou opérationnels. Une description du système sert à cerner les caractéristiques du produit, du service ou de l'activité afin que la GRS et l'assurance de la sécurité puissent être efficaces.

9.7.1.2 La plupart des organisations sont constituées d'un réseau complexe d'interfaces et d'interactions entre différents services internes ainsi qu'avec différentes organisations externes, qui contribuent toutes à l'exploitation sûre de l'organisation. L'utilisation d'une description du système permet à l'organisation d'avoir une idée claire de ses nombreuses interactions et interfaces. La description de celles-ci permettra de mieux gérer les risques de sécurité et les mesures de maîtrise des risques de sécurité et de comprendre l'incidence de changements apportés aux processus et procédures du SGS.

9.7.1.3 Lorsque l'on envisage une description de système, il est important de comprendre qu'un « système » est un ensemble de choses qui fonctionnent ensemble comme des éléments d'un réseau interconnecté. Dans un SGS, ce sont les produits, individus, processus, procédures, installations, services et autres aspects (y compris des facteurs externes) qui sont liés à et peuvent avoir une incidence sur les activités de l'organisation en matière de sécurité de l'aviation. Souvent, un « système » est un ensemble de systèmes, qui peuvent aussi être perçus comme des systèmes de sous-systèmes. Ces systèmes et leurs interactions mutuelles constituent les sources de dangers et contribuent à la maîtrise des risques de sécurité. Les systèmes importants incluent à la fois ceux qui pourraient avoir une incidence directe sur la sécurité de l'aviation et ceux qui touchent l'aptitude et la capacité d'une organisation à assurer une gestion efficace de la sécurité.

9.7.1.4 Une présentation générale de la description du système et des interfaces du SGS devrait être incluse dans la documentation relative au SGS. Une description du système peut inclure une liste de points avec des références aux politiques et procédures. Une présentation graphique, sous la forme d'un diagramme des processus ou d'un organigramme annoté de l'organisation, peut être suffisante pour certaines organisations. Les organisations devraient utiliser une méthode et un format qui leur conviennent.

9.7.1.5 Étant donné que chaque organisation est unique, il n'existe pas de méthode universelle pour la mise en œuvre du SGS. Chaque organisation est censée mettre en œuvre un SGS adapté à sa situation très spécifique. Chaque organisation devrait définir pour elle-même comment elle entend respecter les exigences fondamentales. Pour ce faire, il est important que chaque organisation prépare une description du système qui identifie ses structures organisationnelles, processus et arrangements commerciaux qu'elle considère comme importants pour les fonctions de gestion de la sécurité. Sur la base de la description du système, l'organisation devrait identifier ou élaborer des politiques, processus et procédures qui établissent ses propres exigences en matière de gestion de la sécurité.

9.7.1.6 Lorsqu'une organisation choisit de procéder à un changement significatif ou substantiel des processus identifiés dans la description du système, ces changements devraient être considérés comme pouvant affecter son évaluation de référence des risques de sécurité. En conséquence, la description du système devrait être réexaminée dans le cadre de la gestion des processus de changement.

9.7.2 Gestion des interfaces

Les interfaces ont une incidence sur les risques de sécurité auxquels les prestataires de services sont confrontés. Les interfaces peuvent être internes (p. ex. entre services) ou externes (p. ex. avec d'autres prestataires de services ou avec des sous-traitants). En identifiant et gérant ces interfaces, le prestataire de services aura une meilleure maîtrise de tout risque de sécurité lié à ces interfaces. Ces dernières devraient être définies dans la description du système.

9.7.3 Identification des interfaces du SGS

9.7.3.1 Initialement, les prestataires de services devraient se concentrer sur les interfaces liées à leurs activités commerciales. L'identification de ces interfaces devrait être détaillée dans la description du système qui expose la portée du SGS et devrait inclure les interfaces internes et externes.

9.7.3.2 La Figure 9-3 illustre comment un prestataire de services pourrait cartographier les différentes organisations avec lesquelles il interagit pour identifier toute interface du SGS. L'objectif de cet examen est de produire une liste exhaustive de toutes les interfaces. Cet exercice se justifie par le fait qu'il peut exister des interfaces du SGS dont une organisation n'a pas nécessairement conscience. Dans le cas de certaines interfaces, il se peut qu'il n'y ait pas d'arrangements formels en place, notamment avec des entreprises de distribution d'électricité ou de maintenance de bâtiments.

9.7.3.3 Certaines interfaces internes peuvent concerner des domaines d'activités non directement liés à la sécurité, tels que le marketing, les finances, le droit et les ressources humaines. En effet, ces domaines peuvent avoir une incidence sur la sécurité en raison de décisions prises qui affectent les ressources internes et les investissements, ou d'arrangements et de contrats conclus avec des organisations externes, sans nécessairement aborder la sécurité.

9.7.3.4 Une fois que les interfaces du SGS ont été identifiées, le prestataire de services devrait examiner leur criticité. Cela permet au prestataire de services de prioriser la gestion des interfaces les plus critiques et de leurs risques de sécurité potentiels. Voici quelques points dont il faut tenir compte :

a) Que fournit-on ?

b) Pourquoi est-ce nécessaire ?

c) L'organisation concernée a-t-elle un SGS ou un autre système de gestion en place ?

d) L'interface implique-t-elle le partage de données/d'informations de sécurité ?

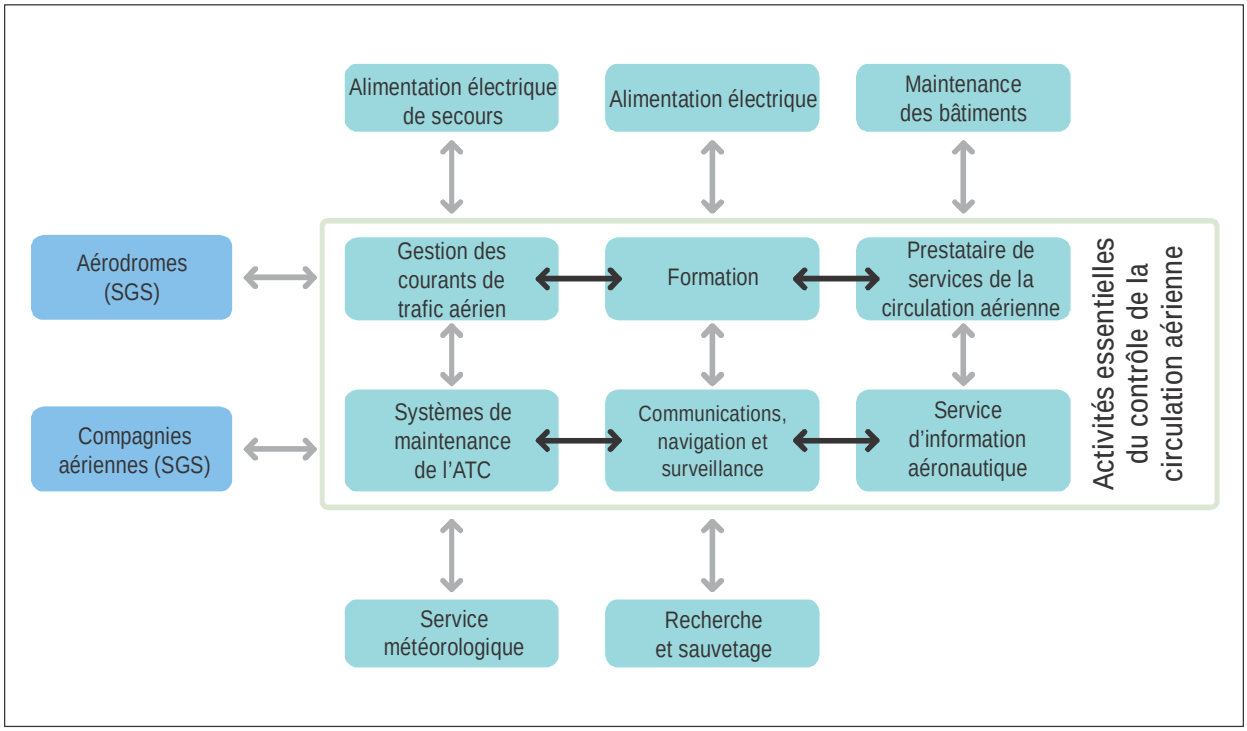

Figure 9-3. Exemple d'interfaces du SGS d'un prestataire de services de la circulation aérienne

Évaluation de l'incidence des interfaces sur la sécurité

9.7.3.5 Le prestataire de services devrait identifier tout danger lié aux interfaces et effectuer une évaluation des risques de sécurité en utilisant ses processus existants d'identification des dangers et d'évaluation des risques de sécurité.

9.7.3.6 Sur la base des risques de sécurité identifiés, le prestataire de services peut envisager de collaborer avec l'autre organisation pour déterminer et définir une stratégie appropriée de maîtrise des risques de sécurité. La collaboration avec l'autre organisation peut permettre de contribuer à identifier des dangers, à évaluer le risque de sécurité ainsi qu'à déterminer la mesure appropriée de maîtrise du risque de sécurité. Cet effort collaboratif est nécessaire parce que la perception des risques de sécurité peut différer d'une organisation à l'autre. La maîtrise des risques devrait être assurée soit par le prestataire de services ou par l'organisation externe.

9.7.3.7 Il importe aussi de reconnaître qu'il incombe à chaque organisation concernée d'identifier et de gérer les dangers qui affectent sa propre organisation. En effet, la criticité de l'interface peut varier d'une organisation à l'autre, chacune pouvant appliquer des classifications différentes des risques de sécurité ou ayant des priorités différentes en matière de risques de sécurité (pour ce qui est des performances de sécurité, des ressources, de la durée, etc.).

Gestion et suivi des interfaces

9.7.3.8 Il incombe au prestataire de services de gérer et de surveiller les interfaces pour s'assurer de la fourniture sûre de ses produits et services. Ainsi, les interfaces seront gérées efficacement et resteront à jour et pertinentes. Des arrangements formels sont un moyen efficace d'y parvenir car les interfaces et les responsabilités qui y sont associées peuvent être clairement définies. Tout changement au niveau des interfaces et ses conséquences devraient être communiqués aux organisations pertinentes.

9.7.3.9 La capacité du prestataire de services à gérer les risques de sécurité aux interfaces se heurte à des difficultés, notamment :

a) les mesures de maîtrise des risques de sécurité d'une organisation ne sont pas compatibles avec celles de l'autre organisation ;

b) la disposition des deux organisations à accepter des changements à leurs propres processus et procédures ;

c) l'insuffisance des ressources ou des savoir-faire techniques disponibles pour gérer et surveiller l'interface ;

d) le nombre et l'emplacement des interfaces.

9.7.3.10 Il est important de reconnaître la nécessité d'une coordination entre les organisations associées à l'interface. Une coordination efficace devrait inclure les points suivants :

a) clarifier les rôles et responsabilités de chaque organisation ;

b) convenir des décisions sur les actions à entreprendre (p. ex. prises de mesures de maîtrise des risques de sécurité et calendriers de mise en œuvre) ;

c) identifier les informations de sécurité qui doivent être partagées et communiquées ;

d) comment et quand la coordination devrait avoir lieu (groupe de travail, réunions régulières, réunions ad hoc ou spécifiques) ;

e) convenir de solutions profitables aux deux organisations mais qui n'entravent pas l'efficacité du SGS.

9.7.3.11 Tous les problèmes de sécurité ou les risques de sécurité liés aux interfaces devraient être documentés et mis à la disposition de chaque organisation pour partage et examen. Cela permettra le partage de leçons tirées et la mise en commun de données de sécurité qui seront utiles aux deux organisations. Des avantages pour la sécurité opérationnelle peuvent être obtenus en renforçant la sécurité atteinte par chaque organisation par une appropriation partagée des risques et responsabilités en matière de sécurité.

9.7.4 Adaptabilité de la portée du SGS

9.7.4.1 Le SGS de l'organisation, y compris ses politiques, processus et procédures, devrait refléter la taille et la complexité de l'organisation et de ses activités. Il devrait tenir compte :

a) de la structure organisationnelle et de la disponibilité de ressources ;

b) de la taille et de la complexité de l'organisation (y compris des sites et bases multiples) ;

c) de la complexité des activités et des interfaces avec des organisations externes.

9.7.4.2 Le prestataire de services devrait effectuer une analyse de ses activités pour déterminer le niveau adéquat de ressources requis pour gérer le SGS. Il devrait aussi déterminer la structure organisationnelle nécessaire pour gérer le SGS. À cet égard, il convient de déterminer qui sera chargé de gérer et tenir à jour le SGS, quels comités de sécurité sont éventuellement nécessaires et s'il faut des spécialistes spécifiques de la sécurité.

Considérations relatives aux risques de sécurité

9.7.4.3 Indépendamment de la taille du prestataire de services, la portée du SGS devrait aussi être adaptée aux risques de sécurité inhérents aux activités du prestataire de services. Même de petites organisations peuvent prendre part à des activités pouvant générer d'importants risques pour la sécurité de l'aviation. C'est pourquoi la capacité de gestion de la sécurité devrait être proportionnelle au risque de sécurité à gérer.

Données de sécurité et informations de sécurité et leur analyse

9.7.4.4 Pour de petites organisations, le faible volume de données peut rendre difficile l'identification de tendances ou de changements dans la performance de sécurité. Il peut dès lors être nécessaire d'organiser des réunions pour soulever des problèmes de sécurité et en discuter avec des experts appropriés. Ce travail peut être plus qualitatif que quantitatif mais il permettra d'identifier des dangers et des risques pour le prestataire de services. Il peut être utile de collaborer avec d'autres prestataires de services ou avec des associations professionnelles car ceux-ci peuvent avoir des données que le prestataire de services n'a pas. Par exemple, de petits prestataires de services peuvent avoir des échanges de vues avec des organisations/exploitants similaires afin de partager des informations sur les risques de sécurité et d'identifier des tendances en matière de performance de sécurité. Les prestataires de services devraient analyser et traiter leurs données internes de façon adéquate même si ces données sont limitées.

9.7.4.5 Les prestataires de services ayant de nombreuses interactions et interfaces devront étudier comment collecter des données de sécurité et des informations de sécurité auprès de multiples organisations. Il se peut qu'ils collectent de grands volumes de données à collationner et analyser ultérieurement. Ces prestataires de services devraient utiliser une méthode appropriée de gestion de ces données. Ils devraient aussi s'intéresser à la qualité des données collectées et à l'utilisation de taxonomies en vue de soutenir l'analyse des données.

9.7.5 Intégration de systèmes de gestion

9.7.5.1 La gestion de la sécurité devrait être considérée comme une partie intégrante d'un système de gestion (et non comme une activité isolée). C'est pourquoi les prestataires de services peuvent mettre en œuvre un système de gestion intégré qui comprend le SGS. Un système de gestion intégré peut être utilisé pour englober des certificats, autorisations ou approbations multiples ou pour couvrir d'autres systèmes de gestion d'entreprise tels que les systèmes de gestion de la qualité, de la sûreté, de la santé au travail et de l'environnement. Le but est d'éliminer les doubles emplois et d'exploiter des synergies en gérant les risques de sécurité de manière transversale pour de multiples activités. Par exemple, lorsqu'un prestataire de services est titulaire de multiples certificats, il peut choisir de mettre en œuvre un seul système de gestion pour couvrir toutes ses activités. Le prestataire de services devrait décider du meilleur moyen d'intégrer ou de scinder son SGS, en fonction des besoins de son entreprise ou de son organisation.

9.7.5.2 Un système de gestion intégré type peut 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) ; de plus amples informations à ce sujet figurent dans le *Manuel de sûreté de l'aviation* (Doc 8973 — Diffusion restreinte) ;

d) un système de gestion de l'environnement (EMS) ;

e) un système de gestion de la santé et de la sécurité au travail (SGSST) ;

f) un système de gestion financière (SGF) ;

g) un système de gestion de la documentation (DMS) ;

h) un système de gestion des risques de fatigue (FRMS).

9.7.5.3 Un prestataire de services peut choisir d'intégrer ces systèmes de gestion sur la base de ses besoins spécifiques. Les processus de gestion des risques et d'audit interne sont des caractéristiques essentielles de la plupart de ces systèmes de gestion. Il convient de reconnaître que les risques et mesures de maîtrise des risques élaborées dans l'un quelconque de ces systèmes pourraient avoir une incidence sur d'autres systèmes. De plus, il peut exister d'autres systèmes opérationnels associés aux activités commerciales qui peuvent aussi être intégrés, tels que la gestion des fournisseurs, la gestion des installations, etc.

9.7.5.4 Un prestataire de services peut aussi envisager d'appliquer le SGS à d'autres domaines pour lesquels la réglementation n'exige pas encore de SGS. Les prestataires de services devraient déterminer le moyen le plus approprié pour intégrer ou scinder leur système de gestion en fonction de leur modèle d'entreprise, de leur environnement d'exploitation, des exigences réglementaires et statutaires ainsi que des attentes de la communauté aéronautique. Quelle que soit l'option retenue, le prestataire de services devrait malgré tout s'assurer qu'il satisfait aux exigences du SGS.

Avantages et difficultés liés à l'intégration de systèmes de gestion

9.7.5.5 L'intégration des différents domaines dans un système de gestion unique améliorera l'efficience en :

a) réduisant les doubles emplois et les chevauchements de processus et de ressources ;

b) réduisant les responsabilités et relations potentiellement conflictuelles ;

c) considérant les incidences plus larges des risques et des possibilités pour toutes les activités ;

d) permettant un suivi et une gestion efficaces de la performance dans toutes les activités.

9.7.5.6 Voici quelques difficultés que peut poser l'intégration de systèmes de gestion :

a) les systèmes existants peuvent avoir des directeurs en fonction différents qui refusent l'intégration ; cela peut entraîner des conflits ;

b) une résistance au changement peut se manifester parmi le personnel visé par l'intégration car celle-ci exigera un renforcement de la coopération et de la coordination ;

c) l'incidence sur la culture générale de la sécurité au sein de l'organisation car il peut exister des cultures différentes, propres à chaque système ; cela pourrait entraîner des conflits ;

d) les réglementations sont susceptibles d'empêcher une telle intégration ou des autorités de réglementation ou des instances de normalisation différentes peuvent avoir des attentes divergentes quant à la façon de satisfaire à leurs exigences ;

e) l'intégration de systèmes de gestion différents (tels qu'un SGQ et un SGS) peut générer un travail supplémentaire pour prouver que les exigences des uns et des autres sont satisfaites.

9.7.5.7 Pour maximiser les avantages de l'intégration et relever les défis qui y sont associés, l'engagement et le leadership de la haute direction sont essentiels pour gérer le changement avec efficacité. Il est important d'identifier la personne chargée de la responsabilité générale du système de gestion intégré.

9.7.6 Intégration d'un SGS et d'un SGQ

9.7.6.1 Certains prestataires de services ont à la fois un SGS et un SGQ. Ces systèmes sont parfois intégrés dans un seul système de gestion. Le SGQ est généralement défini comme la structure organisationnelle et les obligations de rendre compte, ressources, processus et procédures qui y sont associés et sont nécessaires pour établir et promouvoir un système d'assurance de la qualité et d'amélioration en continu tout en fournissant un produit ou un service.

9.7.6.2 Ces deux systèmes sont complémentaires ; le SGS se concentre sur la gestion des risques de sécurité et de la performance de sécurité tandis que le SGQ se concentre sur le respect des règles et exigences normatives afin de répondre aux attentes des clients et aux obligations contractuelles. Les objectifs d'un SGS sont d'identifier les dangers, d'évaluer le risque de sécurité qui y est associé et de mettre en œuvre des mesures efficaces de maîtrise des risques de sécurité. Par contre, le SGQ cible la fourniture constante de produits et services qui répondent à des spécifications pertinentes. Néanmoins, tant le SGS que le SGQ :

a) doivent être planifiés et gérés ;

b) exigent la participation de toutes les fonctions organisationnelles liées à la fourniture de produits et services aéronautiques ;

c) identifient les processus et procédures inefficaces ;

d) visent une amélioration continue ;

e) partagent le même but de fournir des produits et services sûrs et fiables aux clients.

9.7.6.3 Le SGS se concentre sur :

a) l'identification de dangers liés à la sécurité auxquels l'organisation est confrontée ;

b) l'évaluation des risques de sécurité qui y sont associés ;

c) la mise en œuvre de mesures efficaces de maîtrise des risques de sécurité pour atténuer les risques de sécurité ;

d) la mesure de la performance de sécurité ;

e) le maintien d'une affectation appropriée des ressources pour répondre aux exigences en matière de performance de sécurité.

9.7.6.4 Le SGQ se concentre sur :

a) la conformité aux réglementations et exigences ;

b) la constance de la fourniture de produits et services ;

c) le respect des normes de performance spécifiées ;

d) la fourniture de produits et services qui sont « appropriés à l'objectif » et exempts de défauts ou d'erreurs.

9.7.6.5 Le suivi de la conformité aux réglementations est nécessaire pour garantir que le prestataire de services assure une mise en œuvre et un suivi efficaces des mesures de maîtrise des risques de sécurité, appliquées sous la forme de règles. Les causes et facteurs contributifs de toute non-conformité devraient aussi être analysés et traités.

9.7.6.6 Vu les aspects complémentaires du SGS et du SGQ, il est possible d'intégrer ces deux systèmes sans compromettre la fonction de chacun. Leur complémentarité peut se résumer comme suit :

a) le SGS est soutenu par des processus du SGQ tels que les audits, inspections, enquêtes, analyses des causes premières, la conception des processus et les actions préventives ;

b) le SGQ peut identifier des problèmes de sécurité ou des faiblesses dans les mesures de maîtrise des risques de sécurité ;

c) le SGQ peut prévoir des problèmes de sécurité qui existent malgré le respect des normes et spécifications de l'organisation ;

d) les principes, politiques et pratiques en matière de qualité devraient être alignés sur les objectifs de gestion de la sécurité ;

e) les activités du SGQ devraient tenir compte des dangers identifiés et des mesures de maîtrise des risques de sécurité dans la planification et l'exécution des audits internes.

9.7.6.7 En conclusion, dans un système de gestion intégré et aux buts et processus décisionnels unifiés qui tient compte des incidences plus larges dans toutes les activités, les processus de gestion de la qualité et de gestion de la sécurité seront hautement complémentaires et soutiendront la réalisation des objectifs de sécurité généraux.

9.7.7 Analyse des lacunes et mise en œuvre du SGS

9.7.7.1 Avant de mettre en œuvre un SGS, le prestataire de services devrait procéder à une analyse des lacunes. Cette analyse compare les processus et procédures de gestion de la sécurité existants du prestataire de services avec les exigences du SGS telles que déterminées par l'État. Il est probable que le prestataire de services ait déjà mis en place quelques-unes des fonctions du SGS. L'élaboration d'un SGS devrait se baser sur les politiques et processus organisationnels existants. L'analyse des lacunes identifie les lacunes qu'il faudrait combler au moyen d'un plan de mise en œuvre du SGS définissant les actions requises pour mettre en œuvre un SGS pleinement fonctionnel et efficace.

9.7.7.2 Le plan de mise en œuvre du SGS devrait donner une image claire des ressources, tâches et processus requis pour mettre en œuvre le SGS. Le calendrier et l'ordre des tâches du plan de mise en œuvre peuvent dépendre de divers facteurs qui seront spécifiques à chaque organisation, tels que :

a) des exigences réglementaires, statutaires et des clients ;

b) des certificats multiples détenus (avec éventuellement des dates de mise en œuvre réglementaires différentes) ;

c) la mesure dans laquelle le SGS peut s'appuyer sur des structures et processus existants ;

d) la disponibilité de ressources et de budgets ;

e) les interdépendances entre différentes étapes (un système de compte rendu devrait être mis en œuvre avant l'établissement d'un système d'analyse des données) ;

f) la culture de la sécurité existante.

9.7.7.3 Le plan de mise en œuvre du SGS devrait être élaboré en consultation avec le dirigeant responsable et avec d'autres cadres supérieurs, et devrait indiquer qui est responsable des actions à mener ainsi que les calendriers de mise en œuvre. Le plan devrait aborder la coordination avec des organisations externes ou des sous-traitants, selon le cas.

9.7.7.4 Le plan de mise en œuvre du SGS peut être documenté sous différentes formes, allant d'un simple tableur à des logiciels spécialisés en gestion de projets. Ce plan devrait faire l'objet d'un suivi régulier et devrait être actualisé, si nécessaire. Il devrait aussi clarifier quand un élément spécifique peut être considéré comme mis en œuvre avec succès.

9.7.7.5 Tant l'État que le prestataire de services devraient reconnaître qu'il faut plusieurs années avant qu'un SGS ne devienne efficace. Les prestataires de services devraient s'en référer à leur État car celui-ci peut imposer des exigences pour une approche phasée de la mise en œuvre du SGS.

— FIN —

ISBN 978-92-9258-699-7