RÉPUBLIQUE DU CONGO
AGENCE NATIONALE DE L'AVIATION CIVILE

GUIDE RELATIF A LA MISE EN ŒUVRE DU SYSTEME DE GESTION DE LA SECURITE

Réf : G–DSA– 8085–AGA

	Nom	Fonction	Date	Visa
Rédaction	OYOUBA Auguy Marise	**Cheffe de bureau Normes des aérodromes**	01/09/2025	
Vérification	KONDZIKINGUI Brice Nicaise	**Chef de service normes et sécurité des aérodromes**	01/09/2025	
	MOTOLY Arcadius Michel	**Directeur de la Sécurité Aérienne**	02/09/2025	
Validation	MAKAYA BATCHI Roméo Boris	**Responsable Qualité**	03/09/2025	
Approbation	DZOTA Serge Florent	**Directeur Général de l'ANAC**	03/09/2025	

Édition 01 – juin 2017

Niveau de diffusion : ☒ **Interne** ☒ **Externe** ☐ **Confidentiel**

LISTE DE DIFFUSION

N° Copie	Sigle	Destinataire	Format
01	DG	Directeur Général de l'ANAC	P/E
02	DGA	Direction Général Adjoint	P/E
03	CQ	Cellule Qualité	P/E
04	SNSA	Service Normes et Sécurité des Aérodromes	P/E
05	BNA	Bureau Normes des Aérodromes	P/E
06	BSA	Bureau Sécurité des Aérodromes	P/E
07	BAD	Bureau Archives et Documentation	P
08	SNA	Service de la navigation aérienne	P/E
09	AERCO	Direction Générale	P/E
10	ASECNA	Représentation	P/E
11	DIE	Direction des Infrastructures et Equipements	P/E
12	-	Les autres exploitants	P/E
00	DSA	Directeur de la Sécurité Aérienne	P/E
N00		Inspecteurs de supervision de la Sécurité Aérienne AGA	P/E

Observations :

P = Version Papier

E = Version Electronique

N00 = Numéro de la version neutre pour large diffusion

00 = Version originale

LISTE DES PAGES EFFECTIVES

Chapitre	Page	N° d'Édition	Date d'Édition	N° de Révision	Date de Révision
LD	2	01	31 Mai 2017	01	31 Août 2025
LPE	3	01	31 Mai 2017	01	31 Août 2025
ER	4	01	31 Mai 2017	01	31 Août 2025
LR	5	01	31 Mai 2017	01	31 Août 2025
TM	6	01	31 Mai 2017	01	31 Août 2025
I.	7	01	31 Mai 2017	01	31 Août 2025
II.	7	01	31 Mai 2017	01	31 Août 2025
III.	8	01	31 Mai 2017	01	31 Août 2025
IV.	9	01	31 Mai 2017	01	31 Août 2025
V.	9	01	31 Mai 2017	01	31 Août 2025
VI.	10 – 11	01	31 Mai 2017	01	31 Août 2025
VII	12	01	31 Mai 2017	01	31 Août 2025
VIII	13	01	31 Mai 2017	01	31 Août 2025
IX	13 – 14	01	31 Mai 2017	01	31 Août 2025

ENREGISTREMENT DES REVISIONS

N° de Révision	Date d'application	Date d'insertion	Émargement	Remarques
01	Septembre 2025	01/09/2025		Mise à jour des références et de la règlementation nationale en vigueur

LISTE DES RÉFÉRENCES

Référence	Source	Titre	N° Révision	Date de Révision
Arrêté 3007	MTACMM	Conception, exploitation technique et la certification des aérodromes et hélistations		19 août 2025
Doc. 9774	OACI	Manuel de certification des aérodromes	1ère édition	2001
Doc. 9981	OACI	PANS aérodromes	3e édition	2020
Doc 9137-AN/898	OACI	Manuel des services d'aéroport.	1ère Edition	1983
11052	MTACMM	Gestion de la sécurité aérienne		13 juin 2019
Doc	9859	Manuel de gestion de la sécurité	4e édition	2018

TABLE DE MATIERES

I- Généralités

I-1. Objectif et contenu

Le présent guide décrit les caractéristiques essentielles des systèmes de gestion de la sécurité (SGS) et constitue une aide à la mise en œuvre d'un SGS en :

- explicitant la nature des exigences réglementaires ;
- proposant des moyens acceptables de conformité.

Les dispositions de ce guide doivent donc être considérées comme un moyen possible parmi d'autres d'assurer la conformité aux exigences réglementaires.

Ce guide se veut un complément des dispositions de, l'arrêté 11052/MTCAMM-CAB du 13 juin 2019 : Gestion de la sécurité, de manière à adapter la mise en œuvre du SGS à la taille, la complexité et à la nature des activités de l'entreprise ou de l'organisme. On y trouvera matière à enrichir progressivement la démarche de gestion de la sécurité en fonction de l'état d'avancement des travaux sur le SGS. L'ANAC prendra en compte les commentaires qui lui seront transmis ainsi que l'expérience acquise par les entreprises et les organismes pour mettre à jour ce guide et le faire évoluer.

Il présente les exigences pour la mise en place d'un SGS et leur interprétation possible de manière à aider les entreprises et les organismes à les mettre en œuvre.

Les encadrés insérés dans le texte définissent les critères qui seront utilisés pour évaluer le système à des fins d'approbation ou de maintien du respect des exigences réglementaires du SGS.

Les différentes annexes développent de manière approfondie des notions particulières abordées dans ce guide.

I-2. Système de gestion de la sécurité (SGS)

Le SGS a d'abord pour objectif de mettre en place une approche intégrée de la sécurité en assure la cohérence de tous ces éléments afin de fournir au dirigeant responsable les informations de sécurité nécessaires à la prise de décision au sein de l'entreprise ou de l'organisme. De plus, le SGS dépasse la simple conformité réglementaire en prenant en compte les effets de l'adaptation de l'entreprise ou de l'organisme et des acteurs à la variabilité des situations opérationnelles rencontrées pour remplir leurs fonctions.

Enfin, le SGS intègre non seulement une gestion réactive (analyse des évènements) et proactive (processus de traitement du retour d'expérience) de la sécurité mais aussi une approche « prédictive » qui recherche dans l'activité opérationnelle normale, les bonnes pratiques professionnelles et les indicateurs des évolutions non souhaitées de ces pratiques.

Ainsi le SGS repose sur quatre piliers, tel qu'il est défini dans le cadre SGS de l'Organisation de l'Aviation Civile Internationale (OACI). Ce cadre est destiné à constituer un guide rationnel pour l'élaboration et la mise en œuvre du SGS d'un fournisseur de services.

Il faut, en premier lieu, s'assurer que l'ensemble des outils est en place et fonctionne : C'est le premier pilier d'un SGS « Politique et objectifs de sécurité ». Cette exigence implique une volonté exprimée du dirigeant responsable, des moyens, une structure au sein de l'entreprise ou de l'organisme et l'assurance que les données récoltées seront uniquement utilisées à des fins de sécurité.

Le pilier « Gestion du Risque » vise à empêcher les évènements ultimes (accidents, incidents graves). Pour cela on identifie les dangers qui mènent à des évènements indésirables que l'on veut éviter ou réduire.

L'entreprise recueille les informations sur l'apparition de ces évènements indésirables.

Il définit les actions qui lui permettent de les contrôler, c'est-à-dire de maintenir le risque à un niveau acceptable, le plus faible que l'on puisse raisonnablement atteindre.

Le pilier « Assurance du maintien de la Sécurité » consiste à mesurer de manière continue l'efficacité du SGS, au travers d'indicateurs pertinents qui rendent compte du niveau de sécurité et du niveau de maîtrise du risque (effets des actions conduites). Une mise à jour des évènements surveillés est menée dans ce cadre.

Enfin, le dernier pilier est la « Promotion de la sécurité ». Il comprend la diffusion des leçons tirées des analyses du SGS, la formation et l'information de l'ensemble des personnels ainsi que l'amélioration globale de la sécurité du transport aérien, notamment au travers du partage des bonnes pratiques.

1. Politique et objectifs de sécurité
    - 1.1 Engagement et responsabilité de la direction
    - 1.2 Responsabilités en matière de sécurité
    - 1.3 Nomination du personnel clé de sécurité
    - 1.4 Coordination de la planification des interventions en cas d'urgence
    - 1.5 Documentation du SGS
2. Gestion des risques de sécurité
    - 2.1 Identification des dangers
    - 2.2 Évaluation et atténuation des risques de sécurité
3. Assurance de la sécurité
    - 3.1 Surveillance et mesure de la performance de sécurité
    - 3.2 Gestion du changement
    - 3.3 Amélioration continue du SGS
4. Promotion de la sécurité
    - 4.1 Formation et éducation
    - 4.2 Communications de sécurité.

Figure 1 : Cadre SGS de l'OACI

I-3. Description du système

Une description du système est la première condition requise pour établir un SGS dans une organisation. Chaque système contient des vulnérabilités intrinsèques potentielles de la sécurité, qui sont caractérisées en termes de dangers. Le processus d'identification des dangers ne peut identifier que les dangers qui entrent dans le champ de la description du système. Il faut donc que les limites du système, selon sa description formelle, soient suffisamment larges pour englober tous les dangers auxquels il pourrait être confronté ou qu'il pourrait générer. Il importe en particulier que la description comprenne les interfaces au sein du système, ainsi que les interfaces avec les systèmes plus vastes dont fait partie le système évalué.

Une description détaillée du système devrait inclure:

a) le rôle du système ;
b) comment le système sera utilisé ;
c) les fonctions du système ;
d) les limites du système et les interfaces externes ;
e) le contexte dans lequel le système fonctionnera.

Les conséquences en matière de sécurité d'une perte ou d'une dégradation potentielle du système seront déterminées, en partie, par les caractéristiques du contexte opérationnel dans lequel le système sera intégré. La description du contexte devrait donc inclure tous les facteurs qui pourraient avoir un effet significatif sur la sécurité. Ces facteurs, qui varieront d'une organisation à une autre, pourraient comprendre, par exemple, les caractéristiques du trafic aérien et terrestre, l'infrastructure des aérodromes et les facteurs liés aux conditions météorologiques. La description du système devrait porter aussi sur les procédures d'urgence et autres opérations non normales, par exemple une défaillance des communications ou des aides de navigation.

Un exemple détaillé de description systémique d'un aérodrome est donné dans le D-DSA-8085-AGA.

I-4. Analyse d'écarts

La mise en œuvre d'un SGS exige qu'un prestataire de services procède à une analyse de son système pour déterminer quelles composantes et quels éléments d'un SGS sont actuellement en place et lesquels il faut ajouter ou modifier pour répondre aux besoins de la mise en œuvre. Cette

analyse, appelée analyse d'écarts, fait intervenir une comparaison des besoins du SGS avec les ressources existantes du prestataire de services.

L'analyse d'écarts fournit, sous forme de liste de vérification, des informations qui aideront à évaluer les composantes et les éléments qui constituent le cadre SGS de l'OACI et à identifier ceux qu'il faudra développer. Une fois que l'analyse d'écarts sera réalisée et documentée, elle constituera une base du plan de mise en œuvre du SGS.

La liste de vérification exposée en C-DSA-8086-AGA peut servir de modèle pour effectuer une analyse d'écarts.

II- Engagement de la direction

II-1 Politique de sécurité

Le point de départ pour assurer l'efficacité et l'efficience du SGS d'une organisation est la politique de sécurité de l'organisation, élaborée par sa haute direction et signée par le Dirigeant responsable.

Le fascicule (D-DSA-8087-AGA) présente un exemple de politique de sécurité. En termes généraux, celle-ci doit comprendre un engagement à :

a) appliquer les plus hautes normes de sécurité ;
b) observer toutes les prescriptions légales et les normes internationales applicables, et les meilleures pratiques effectives ;
c) apporter toutes les ressources appropriées ;
d) faire de l'application de la sécurité une responsabilité première de tous les cadres ;
e) s'assurer que la politique est comprise, appliquée et maintenue à tous les niveaux.

Une fois élaborée, la politique de sécurité doit être communiquée par la haute direction à tout le personnel, avec une approbation visible. La politique de sécurité du dirigeant responsable s'applique également à ses sous-traitants pour les activités qui les concernent.

Critères d'évaluation

• Il existe une politique de sécurité, et celle-ci est adaptée à la taille et à la complexité de l'organisme.
• La politique de sécurité est signée par le dirigeant responsable
• La politique de sécurité énonce les intentions, les principes de gestion et l'engagement de l'organisme visant à l'amélioration continue du niveau de sécurité.
• Le dirigeant responsable approuve la politique de sécurité.
• Le dirigeant responsable fait la promotion de la politique de sécurité.
• La politique de sécurité est examinée de façon périodique.
• Le personnel, quel que soit son niveau dans l'organisme, participe à l'établissement et au maintien du système de gestion de la sécurité.
• La politique de sécurité est communiquée à tous les employés dans le but que ceux-ci soient

conscients de leurs obligations personnelles en matière de sécurité.

II.2 Objectifs de sécurité

C'est aussi la haute direction qui doit établir des objectifs de sécurité, ainsi que les normes de performance de sécurité pour le SGS, et donc pour l'organisation dans son ensemble. Les objectifs de sécurité doivent identifier ce que l'organisation veut accomplir, en termes de gestion de la sécurité, et déterminer les étapes à suivre pour réaliser les objectifs. Les normes de performance de sécurité permettent de mesurer le comportement de l'organisation vis-à-vis de la performance de sécurité, et donc vis-à-vis de la gestion de la sécurité. Aussi bien les objectifs de sécurité que les normes de performance de sécurité doivent être liés aux indicateurs de performance de sécurité, aux cibles de performance de sécurité et aux plans d'action du SGS.

Les objectifs de sécurité peuvent prendre la forme d'un bref énoncé décrivant en termes généraux les attentes de l'organisation. Dans certains cas, cet énoncé peut être incorporé à l'énoncé de politique de sécurité de la rubrique II.1, ci-dessus. Les buts propres au rendement sont des buts précis et mesurables qui vous permettent de mesurer le niveau de réussite du SGS.

Par ailleurs, la définition des objectifs se base sur une identification des risques sur le terrain. Une fois les risques identifiés, les objectifs pertinents peuvent être définis pour l'organisation. Il s'agit d'identifier les points nécessitant un suivi particulier dans un souci d'amélioration de la sécurité. En fonction de la spécificité de chaque fournisseur, les objectifs seront différents et plus ou moins nombreux d'un organisme à l'autre.

Dans un premier temps, les objectifs de sécurité peuvent être qualitatifs.

A terme, des valeurs cibles devront être définies en fonction de la situation sur le terrain. Les valeurs cibles sont des objectifs chiffrés définis pour les objectifs de sécurité. Les valeurs cibles peuvent être exprimées en pourcentage ou en valeur absolue.

Critères d'évaluation

• Des objectifs de sécurité ont été établis.

• Les objectifs de sécurité sont exprimés sous la forme d'un énoncé de première importance précisant que l'organisme s'engage à améliorer la sécurité.

• Il y a un processus formel permettant de développer un ensemble cohérent de buts propres à la sécurité nécessaires à l'atteinte des objectifs.

• Les objectifs et les buts propres à la sécurité sont publiés et diffusés.

• Des ressources ont été allouées à l'atteinte des objectifs et des buts.

• Il y a un processus formel permettant de développer et de tenir à jour un ensemble de paramètres de rendement mesurables.

III-Personnel et Responsabilités de sécurité

III-1. Dirigeant responsable

L'organisation doit identifier le Dirigeant responsable, qui doit être une personne unique, identifiable, ayant la responsabilité finale de la performance efficace et efficiente du SGS de l'organisation.
Selon la taille de l'organisation et sa complexité, il peut être :

a) le président directeur général ;
b) le président de directoire ;
c) le directeur général ;
d) le président du conseil d'administration ;
e) un associé ; ou
f) le propriétaire.

III-2. Gestionnaire de la sécurité

Le fournisseur de service désigne une fonction, indépendante de l'encadrement opérationnel, rattachée au dirigeant responsable, et chargée de la mise en œuvre du SGS (développement, animation, évolution).
La personne qui exerce cette fonction, que l'on désignera ci-après Gestionnaire de la sécurité, ne doit pas être un agent opérationnel et doit être indépendante de l'encadrement opérationnel car la fonction de gestion de la sécurité ne peut pas être juge (en tant que fonction qui analyse la sécurité) et partie (en tant qu'acteur ayant un rôle direct dans la sécurité).
La position du responsable SGS dans l'organisation doit lui permettre d'avoir accès à toutes les activités entra dans le périmètre du SGS.
Dans un environnement SGS, le gestionnaire de la sécurité est la personne responsable de la collecte et de l'analyse des données de sécurité sur les dangers, ainsi que de la diffusion, aux cadres hiérarchiques, des renseignements sur les dangers et sur les risques de sécurité des conséquences de dangers. Pour cette raison, les critères de sélection pour un gestionnaire de la sécurité acquièrent une importance particulière et devraient comprendre notamment les qualifications suivantes :

a) expérience de la gestion opérationnelle ;
b) bagage technique pour comprendre les systèmes qui appuient les opérations ;
c) compétences humaines ;
d) compétences analytiques et de résolution de problèmes ;
e) compétences en gestion de projets ;
f) compétences en communications orales et écrites.

Dans le cas où un système qualité est déjà mis en place sur la plate-forme, le responsable qualité peut être responsable SGS, tout en restant attentif à la charge de travail générée par les actions portant spécifiquement sur la sécurité.

Dans le cas où un exploitant gère plusieurs organismes de fourniture de service, il est possible que le responsable SGS soit en charge du SGS sur ces différentes sites de fourniture de service.

Une description de poste type pour un directeur de la sécurité figure dans le fascicule D-DSA-8088-AGA du présent document.

Cas particulier des organisations de petites tailles :

Dans le cas où la taille de l'organisation ne permet pas d'assurer l'indépendance de la fonction chargée de la mise en œuvre du SGS, des solutions différentes et dérogeant partiellement à ce principe peuvent être définies.

Sont considérées comme étant « des organisations de petite taille » :

• Les entreprises de transport aérien public n'employant pas plus de 20 personnes à plein temps exécutant des tâches opérationnelles.

• les organismes de gestion du maintien de navigabilité comprenant un maximum de 5 personnels à plein temps exécutant des tâches de maintien de navigabilité.

• Les organismes d'entretien comprenant un maximum de 10 personnes à plein temps exécutant des tâches de maintenance.

• Les aérodromes qui ont accueilli moins de 10 000 mouvements d'aéronefs de plus de 5,7 tonnes au cours de l'une des trois dernières années civiles écoulées.

Ainsi pour les organismes concernés, il est envisageable :

• Que le dirigeant responsable soit également le responsable SGS (ou assure certaines fonctions SGS) ; ou

• Que le responsable SGS fasse partie de l'encadrement opérationnel.

Dans ce sens, le lien fonctionnel existant entre le dirigeant responsable et le responsable SGS apparaît explicitement dans l'organigramme. Toutefois, certaines tâches ne peuvent être réalisées par les agents parties prenantes, notamment le pilotage de l'analyse des évènements de sécurité de la réalisation des audits internes pour les missions qui leur incombent. Il est par exemple possible de :

• Faire appel à des agents d'un autre fournisseur de service pour l'analyse des évènements ou la réalisation des audits internes, sous réserve que leurs compétences dans le domaine soient avérées ;

• Faire appel à des agents de l'organisation pour l'analyse d'un évènement, sous réserve qu'ils ne soient pas concernés par l'évènement et que leurs compétences dans le domaine avérées ;

• Faire appel à des personnes ou société extérieures pour l'analyse des évènements ou la réalisation des audits internes, sous réserve que leurs compétences dans le domaine soient avérées ;

Toutefois, malgré l'externalisation de ces tâches l'exploitant d'aérodrome reste responsable de la gestion de la sécurité sur la plate-forme.

III-3. Responsabilités en matière de sécurité

Afin d'identifier la contribution des différents acteurs mais aussi des procédures, des ressources disponibles et de la structure de l'organisation dans les analyses de sécurité, les personnels

d'encadrement doivent connaitre leurs responsabilités en matière de sécurité, lesquelles doivent être formalisées.

Ceci peut être réalisé à travers l'inclusion dans la description de poste de chaque cadre supérieur (chef de service ou responsable d'unité fonctionnelle), dans la mesure appropriée, des responsabilités concernant le fonctionnement du SGS, en plus des responsabilités spécifiques pour le fonctionnement du service ou de l'unité fonctionnelle.

Dans de nombreux cas, cette description pourrait être rendue plus explicite par la présence d'un organigramme.

Dans tous les cas, l'organisme doit disposer d'un organigramme mentionnant au minimum le dirigeant responsable du fournisseur, le responsable du SGS et les agents de l'organisation ayant des fonctions dans le domaine de la sécurité. Le dirigeant responsable et le responsable SGS sont désignés nominativement. Il convient également de faire apparaître dans l'organigramme toutes les structures impliquées dans le SGS.

Exemple : Si les aspects relatifs à la formation des personnels sont traités au sein d'une entité « Ressources Humaines » de l'organisme, il convient de le mentionner dans l'organigramme.

Dirigeant responsable

La responsabilité finale en matière de sécurité incombe au dirigeant responsable.

Ce dernier est responsable :

- De la définition et de la mise en œuvre de la politique de sécurité de l'organisation ;
- De la définition des responsabilités des personnels ;
- De la définition et du respect des objectifs de sécurité ;
- De la désignation d'un responsable chargé de la mise en œuvre du SGS ;
- De la présidence de la revue de sécurité et de l'animation du comité de sécurité ;

Gestionnaire de la sécurité

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

a) gérer le plan de mise en œuvre du SGS au nom du Dirigeant responsable ;
b) exécuter/faciliter l'identification des dangers et l'analyse des risques de sécurité ;
c) surveiller les mesures correctives et évaluer leurs résultats ;

d) présenter des rapports périodiques sur la performance de sécurité de l'organisation ;
e) tenir les dossiers et la documentation de sécurité ;
f) planifier et organiser la formation du personnel en matière de sécurité ;
g) donner des avis indépendants sur les questions de sécurité ;
h) surveiller les préoccupations de sécurité dans l'industrie de l'aviation et leur impact perçu sur les opérations de l'organisation visant à la fourniture de services ;
i) coordonner et communiquer (au nom du Dirigeant responsable) avec l'autorité nationale de supervision et les autres agences de l'État, selon les besoins, au sujet des questions relatives à la sécurité ;
j) coordonner et communiquer (au nom du Dirigeant responsable) avec les agences internationales au sujet des questions relatives à la sécurité.

Fonctions d'encadrement :

Les responsabilités des personnes assurant des fonctions d'encadrement sont notamment les suivantes:

• Veiller à ce que la fonction de suivi de la sécurité soit mise en œuvre dans leur service ;
• Veiller à l'application des procédures d'évaluation et d'atténuation des risques concernant leur service/division;
• S'assurer que les personnels sous leur autorité ont suivi les formations adéquates ;
• Faire remonter au responsable SGS toute information pertinente nécessaire à l'accomplissement de ses tâches ;
• Mettre en œuvre les actions préventives et correctives relevant de leur service ;

Personnels en charge de tâches opérationnelles :

Leurs responsabilités comprennent notamment celles:

• D'exercer leurs tâches dans le respect de la réglementation ;
• De respecter la politique de sécurité de l'exploitant ;
• De notifier les évènements liés à la sécurité ;
• Faire remonter au responsable SGS toute information pertinente nécessaire à l'accomplissement de ses tâches ;
• De prendre connaissance des enseignements de sécurité diffusée et d'en tenir compte.

Critères d'évaluation

• Il y a eu nomination d'un gestionnaire supérieur responsable chargé de veiller à ce que le système de gestion de la sécurité a été mis en œuvre correctement et fonctionne conformément aux exigences dans tous les domaines de l'organisme.
• Les pouvoirs, les responsabilités et les obligations en matière de sécurité visant le personnel à tous

les niveaux de l'organisme sont définis et documentés.

• Les pouvoirs, les responsabilités et les obligations en matière de sécurité sont examinés après des modifications importantes apportées à l'organisme.

• Les pouvoirs, les responsabilités et les obligations en matière de sécurité sont diffusés à tout le personnel dans la documentation clé et dans les supports de communication.

• Tout le personnel comprend ses pouvoirs, ses responsabilités et ses obligations en ce qui concerne la totalité des processus, des décisions et des mesures en matière de sécurité.

IV-Coordination de la planification d'intervention en cas d'urgence

Un plan d'intervention en cas d'urgence (ERP) indique par écrit les mesures à prendre à la suite d'un accident, en précisant qui sera responsable de chaque action. L'objet d'un ERP est d'assurer une transition ordonnée et efficiente des opérations normales aux opérations d'urgence, y compris la délégation de pouvoirs d'urgence et l'attribution de responsabilités d'urgence. L'autorisation des mesures à prendre par le personnel clé figure aussi dans le plan, ainsi que la coordination des efforts pour faire face à l'urgence.

L'objectif général est de poursuivre les opérations en sécurité ou de retourner dès que possible à des opérations normales.

Il faut que les aéroports élaborent un plan d'urgence d'aérodrome, que les fournisseurs de services de la circulation aérienne élaborent des plans d'urgence et que les compagnies aériennes élaborent un plan d'intervention d'urgence. Étant donné que les opérations des aéroports, du contrôle du trafic aérien et des compagnies aériennes se chevauchent, il est évident que ces plans devraient être compatibles. Leur coordination devrait être décrite dans le manuel SGS.

Un exercice de simulation de crise (scénario d'accident ou incident grave, participation mixte de l'encadrement et des acteurs de première ligne) peut être réalisé avec la participation du dirigeant responsable.

La gestion de crise repose plus souvent sur les qualités du dirigeant responsable et des gestionnaires de crise que sur les processus et outils de gestion de crise procédures, manuels).

On retiendra en particulier que la formation des responsables décisionnels doit porter surtout sur le travail en équipe et sur les contacts préétablis avec les entités susceptibles d'intervenir en cas de crise (internes et externes) ainsi que sur une analyse critique des normes traditionnelles du management qui sont souvent mises en défaut lors d'une crise, au même titre que les procédures.

La formation peut également aborder la mise en situation ou les études de cas, l'implication des responsables sur le terrain, les diverses formes d'accès à l'information, et l'évaluation collective des performances et des décisions.

Critères d'évaluation

• L'organisme a une politique de préparation aux situations d'urgence qui précise les rôles et les responsabilités de chacun en cas d'accident.

• Il existe un processus de notification qui comprend une liste des personnes à appeler en cas d'urgence et un processus de mobilisation interne.

• L'organisme a conclu des ententes ou des accords avec d'autres organismes portant sur une aide mutuelle et sur la fourniture de services d'urgence.

• L'organisme dispose de procédures documentées à suivre en cas d'urgence.

• Il existe une procédure de surveillance du bien-être de toutes les personnes concernées.

• L'organisme dispose d'une procédure pour aviser les proches.

• L'organisme dispose de procédures établies pour gérer les questions de relations avec les médias.

• Il existe des responsabilités d'enquête en cas d'accident bien définies au nom de l'organisme.

• L'exigence visant à la préservation des preuves est clairement énoncée.

• Le personnel concerné reçoit une formation en préparation et en réaction aux situations d'urgence.

• Les procédures de communication avec les agences gouvernementales et de protection de la zone concernée doivent figurer dans la politique de préparation aux situations d'urgence.

• Un plan de récupération d'un aéronef accidenté est mis au point par l'organisme, en collaboration avec les constructeurs et les exploitants d'aéronefs.

• Il existe une procédure de consignation des dossiers en cas d'intervention d'urgence.

• Il existe une procédure traitant des assurances.

V- Documentation SGS

V-1. Plan de mise œuvre du SGS

Le plan de mise en œuvre d'un SGS définit la démarche de gestion de la sécurité de l'organisation. Comme tel, il représente une stratégie réaliste pour la mise en œuvre d'un SGS qui répondra aux objectifs de sécurité de l'organisation tout en appuyant une fourniture efficace et efficiente des services. Il décrit comment une organisation réalisera ses objectifs d'entreprise en matière de sécurité et comment elle répondra à des exigences de sécurité nouvelles ou revues, réglementaires ou autres. Les éléments significatifs de ce plan seront normalement inclus dans le plan d'activités de l'organisation.

Le plan de mise en œuvre d'un SGS, qui peut être constitué de plus d'un document, expose en détail les mesures à prendre, par qui et dans quels délais.

En fonction de la taille de l'organisation et de la complexité de ses opérations, le plan de mise en œuvre du SGS pourra être mis au point par une seule personne ou par un groupe de planification possédant une base d'expérience appropriée. Le groupe de planification devrait se réunir

régulièrement avec la haute direction pour évaluer les progrès du plan de mise en œuvre ; des ressources correspondant à la tâche qui lui incombe devraient lui être attribuées (y compris du temps pour les réunions).

Le contenu type du plan de mise en œuvre d'un SGS est le suivant :

a) politique et objectifs de sécurité ;
b) description du système ;
c) analyse d'écarts ;
d) composantes du SGS ;
e) rôles et responsabilités en matière de sécurité ;
f) politique de compte rendu de dangers ;
g) moyens de faire intervenir les employés ;
h) mesure de la performance de sécurité ;
i) communications relatives à la sécurité ;
j) formation relative à la sécurité ;
k) examen par la direction de la performance de sécurité.

Une fois le plan de mise en œuvre du SGS établi, il doit avoir l'approbation de la haute direction. Un cadre temporel typique pour la mise en œuvre d'un SGS s'étend sur un à quatre ans. Un modèle type d'un plan de mise en œuvre de SGS et le cadre temporel correspondant figurent à l'Annexe5 du présent document.

Critères d'évaluation

• Le plan de mise en œuvre du SGS est entériné par la haute direction de l'organisation.

• Le plan de mise en œuvre du SGS est élaboré sur la base des réglementations nationales, des normes et pratiques recommandées (SARP) internationales, de la description du système et des résultats d'une analyse d'écarts.

• Le plan de mise en œuvre du SGS prévoir une série gérable d'étapes à suivre pour mettre en œuvre un SGS ;

• Une démarche par phases est proposée pour aider à gérer efficacement la charge de travail associée à la mise en œuvre du SGS.

• Chaque phase est basée sur l'introduction de certains éléments spécifiques du cadre SGS de l'OACI.

• Le chronogramme de mise en œuvre de chaque phase doit correspondre à la taille de l'organisation et à la complexité des services fournis.

V-2. Manuel du Système de Gestion de la Sécurité (MSGS)

Le Manuel du Système de Gestion de la Sécurité (MSGS), qui est un instrument clé pour communiquer à toute l'organisation la démarche de sécurité de l'organisation, documente tous les

aspects du SGS, y compris la politique, les objectifs et les procédures de sécurité, et les responsabilités individuelles en matière de sécurité.

Le contenu type d'un MSGS porte sur ce qui suit :

a) portée du manuel de gestion de la sécurité ;
b) politique et objectifs de sécurité ;
c) responsabilités en matière de sécurité ;
d) personnel clé de sécurité ;
e) procédures de contrôle de la documentation ;
f) coordination de la planification des interventions en cas d'urgence ;
g) dispositifs d'identification des dangers et de gestion des risques ;
h) assurance de la sécurité ;
i) surveillance de la performance de sécurité ;
j) audits de sécurité ;
k) gestion du changement ;
l) promotion de la sécurité ;
m) activités sous-traitées.

Critères d'évaluation

• Il existe une documentation consolidée qui décrit le système de gestion de la sécurité ainsi que les relations entre ses divers composants.
• Des manuels ou des moyens électroniques contrôlés servent à documenter le système.
• Ce renseignement se trouve, ou est incorporé par renvoi, dans un document approuvé et contrôlé.
• La documentation consolidée est facilement accessible au personnel.
• Il existe un processus d'examen périodique de la documentation du système de gestion de la sécurité permettant de s'assurer que ladite documentation est toujours adaptée, pertinente et efficace et que les modifications apportées à la documentation de l'entreprise ont été mises en œuvre.

VI-Gestion des risques de sécurité

VI-1.Identification des dangers

La gestion des risques de sécurité commence par une description des fonctions du système, comme base pour l'identification des dangers.

Dans la description du système, ses composantes et leurs interfaces avec son environnement opérationnel sont analysées pour déterminer la présence de dangers, ainsi que pour identifier les contrôles des risques de sécurité déjà existants dans le système, ou en constater l'absence.

Les dangers sont analysés dans le contexte du système décrit, leurs conséquences potentiellement dommageables sont identifiées, et elles sont évaluées pour ce qui est des risques de sécurité.

Lorsqu'il est évalué que les risques de sécurité des conséquences de dangers sont trop élevés pour être acceptables, il faut incorporer dans le système des contrôles additionnels de ces risques. Évaluer la conception du système et vérifier qu'il maîtrise adéquatement les conséquences de dangers constitue donc un élément fondamental de la gestion de la sécurité.

L'identification des dangers est donc la première étape dans un processus formel de collecte, d'enregistrement, de suivi et de rétro-information concernant les dangers et les risques de sécurité de l'exploitation.

Dans un SGS bien déployé, les sources d'identification des dangers doivent inclure les trois méthodes: méthodes réactives, proactives et prédictives.

Une approche structurée de la détermination des dangers assure l'identification, dans toute la mesure du possible, de la plupart des dangers dans le contexte opérationnel du système. Les techniques appropriées pour assurer cette approche structurée pourraient comprendre:

a) Des listes de vérification. Examiner l'expérience et les données disponibles provenant de systèmes similaires et dresser une liste de vérification de dangers. Les zones potentiellement dangereuses exigeront une évaluation plus poussée. ;

b) Examen en groupe. Des sessions de groupe pourraient être utilisées pour examiner la liste de vérification des dangers, procéder à de plus larges remue-méninges sur les dangers ou mener une analyse de scénarios détaillée.

Les sessions d'identification de dangers exigent une équipe de personnel opérationnel et technique expérimenté et sont généralement menées dans le cadre d'une certaine forme de débat de groupe dirigé. Un facilitateur familiarisé avec les techniques de remue-méninges devrait gérer les sessions de groupe. Un gestionnaire de la sécurité, s'il est nommé, jouerait normalement ce rôle. C'est dans le contexte de l'identification des dangers que ces sessions de groupe sont ici évoquées, mais le même groupe s'occuperait aussi de l'évaluation de la probabilité et de la sévérité des risques de sécurité des conséquences de dangers identifiés.

L'évaluation des dangers devrait prendre en considération toutes les possibilités, de la moins probable à la plus probable. Il faut tenir compte adéquatement des situations représentant le « pire des cas », mais il importe aussi que les dangers à inclure dans l'analyse finale soient des dangers « crédibles ». Il est souvent difficile de définir la limite entre le pire des cas crédible et un cas tellement dépendant de coïncidences s'il ne devrait pas en être tenu compte.

Les définitions suivantes peuvent servir de guide pour prendre de telles décisions :

a) Pire des cas. Les conditions les plus défavorables à prévoir, par exemple niveaux de trafic extrêmement élevés ou perturbations météorologiques extrêmes ;

b) Cas crédible. Ceci implique qu'il ne soit pas déraisonnable de prévoir que la combinaison supposée de conditions extrêmes se produira dans le cycle de vie opérationnel du système.

Tous les dangers identifiés devraient se voir attribuer un numéro de danger et être enregistrés dans une fiche de dangers. La fiche de dangers devrait contenir une description de chaque danger, de ses conséquences, de l'évaluation de la probabilité et de la gravité des risques de sécurité des

conséquences, ainsi que des contrôles nécessaires des risques de sécurité, qui seront le plus généralement des mesures d'atténuation. La fiche de dangers devrait être actualisée à mesure que de nouveaux dangers sont identifiés et que de nouveaux contrôles des risques de sécurité (c'est-à-dire de nouvelles mesures d'atténuation) sont proposés.

VI-2. Evaluation et atténuation du risque de sécurité

Une fois les dangers identifiés, les risques de sécurité de leurs conséquences potentielles doivent être évalués. L'évaluation des risques de sécurité est l'analyse des risques de sécurité des conséquences de dangers dont il a été déterminé qu'ils menacent les capacités d'une organisation. Les analyses de risques de sécurité utilisent une répartition classique des risques en deux composantes — la probabilité d'occurrence d'un événement ou d'une situation dommageable, et la gravité de l'événement ou de la situation, le cas échéant. La prise de décision et l'acceptation en ce qui concerne le risque de sécurité sont spécifiées en utilisant une matrice d'acceptation du risque. Il faut une matrice, mais il faut aussi du discernement. Il convient que la définition et la construction finale de la matrice soient laissées à l'organisation du prestataire de services, pour conception, et soient soumises à l'approbation de la DAC. Cela pour assurer que chaque organisation utilise, en matière de sécurité, des outils décisionnels pertinents pour ses opérations et son contexte opérationnel, eu égard à la vaste diversité dans ce domaine.

Après l'évaluation des risques de sécurité à l'étape précédente, il faut procéder à l'élimination et/ou à l'atténuation jusqu'au niveau « le plus faible que l'on puisse raisonnablement atteindre » [ALARP - As low as reasonably practicable]. C'est ce qu'on appelle atténuation des risques de sécurité. Des contrôles des risques de sécurité doivent être conçus et mis en œuvre. Il peut s'agir de procédures additionnelles ou modifiées, de nouveaux moyens de supervision, de modifications de la formation, d'équipement supplémentaire ou modifié, ou de toute autre option d'élimination/atténuation. Presque invariablement, ces alternatives comporteront le déploiement ou le redéploiement de l'une des trois défenses traditionnelles en aviation (technologie, formation, réglementation) ou de combinaisons de ces défenses. Après la conception des contrôles des risques de sécurité, mais avant la « mise en service» du système, il faut évaluer s'ils introduisent de nouveaux dangers pour le système.

À ce stade, le système est prêt pour le déploiement/redéploiement opérationnel, en supposant que les contrôles des risques de sécurité soient jugés acceptables. La composante suivante du SGS, l'assurance de la sécurité, utilise des techniques d'audit, d'analyse, d'examen et similaires, correspondant à celles qui sont utilisées par les systèmes de gestion de la qualité. Ces techniques sont utilisées pour surveiller les contrôles des risques de sécurité afin de s'assurer qu'ils continuent d'être mis en œuvre selon leur conception et continuent d'être efficaces dans le contexte opérationnel dynamique.

Le modèle de la matrice d'évaluation et d'atténuation des risques de l'OACI est donné à titre d'exemple en annexe 6.

Critères d'évaluation

• Il existe un processus structuré qui permet d'évaluer le risque associé aux dangers identifiés, risque exprimé en fonction de la gravité, du niveau d'exposition et de la probabilité de l'événement.

• Il existe un critère d'évaluation des risques et du niveau tolérable de risques que l'organisme est prêt à accepter.

• L'organisme dispose de stratégies de contrôle des risques qui comprennent des plans de mesures correctives et préventives dans le but d'éviter la récurrence d'événements et de lacunes déjà signalés.

• L'organisme dispose d'un processus d'évaluation de l'efficacité des mesures correctives ou préventives qui ont été développées.

• Les mesures correctives ou préventives, y compris les échéances dans le temps, sont documentées.

VII- Assurance de la sécurité

VII-1. Surveillance et mesure de la performance en matière de sécurité

La tâche première de l'assurance de la sécurité est le contrôle. Celui-ci est réalisé au travers de la surveillance et du suivi de la performance de sécurité, processus par lequel la performance de sécurité de l'organisation est vérifiée par rapport à la politique de sécurité et aux objectifs de sécurité approuvés. Le contrôle de l'assurance de la sécurité est réalisé par la surveillance et la mesure des résultats des activités auxquels le personnel opérationnel doit se livrer pour la fourniture de services par l'organisation.

On trouvera ci-après une liste d'aspects ou domaines génériques à considérer pour « assurer la sécurité » par la surveillance et la mesure de la performance de sécurité :

a) Responsabilité. À qui incombe la responsabilité de gérer les activités opérationnelles (planification, organisation, direction, contrôle) et leur accomplissement ultime ;

b) Autorité. Qui peut (et qui ne peut pas) diriger, contrôler ou modifier les procédures, et qui peut prendre les décisions clés telles que les décisions d'acceptation d'un risque de sécurité ;

c) Procédures. Modes spécifiés d'exécution des activités opérationnelles, traduisant le « quoi » (objectifs) en « comment » (activités pratiques) ;

d) Contrôles. Éléments du système, comprenant matériel, logiciel/documentation, procédures spéciales ou étapes procédurales, et pratiques de supervision pour maintenir les activités opérationnelles sur la bonne voie ;

e) Interfaces. Examen d'éléments tels que les lignes d'autorité entre départements/services, la cohérence des procédures, et une détermination claire des responsabilités entre organisations, unités de travail et employés ;

f) Éléments de mesure du processus. Moyens d'apporter aux parties responsables un retour d'information les informant que les dispositions nécessaires sont prises, que les outputs requis sont produits et que les résultats attendus sont réalisés.

L'information relative à la performance de sécurité et à sa surveillance provient de diverses sources, dont les audits et évaluations formels, les enquêtes sur des événements liés à la sécurité, la surveillance continue des activités quotidiennes relatives à la fourniture de services, et les apports d'employés au moyen des systèmes de comptes rendus de dangers. Chacun de ces types de sources d'information peut exister dans une certaine mesure dans chaque organisation. Cependant, les spécifications sur ce que ces sources devraient être ou ce à quoi elles devraient « ressembler », devraient être laissées à un niveau opérationnel, ceci permettant aux différentes organisations de les adapter à la portée et à l'échelle appropriées au type d'organisation et à sa taille. Les sources d'information pour la surveillance et la mesure de la performance de sécurité sont notamment :

a) comptes rendus de dangers ;
b) études sur la sécurité ;
c) examens de la sécurité ;
d) audits ;
e) enquêtes sur la sécurité ;
f) investigations internes sur la sécurité.

Les comptes rendus de dangers et les systèmes de comptes rendus de dangers sont des éléments essentiels dans l'identification des dangers. Personne ne connaît mieux la performance réelle d'un système que le personnel opérationnel. Une organisation qui souhaite savoir comment le système fonctionne réellement au quotidien, par opposition à comment il devrait fonctionner selon « le livre », devrait interroger le personnel opérationnel, d'où l'importance des systèmes de comptes rendus. Il existe trois types de systèmes de comptes rendus :

a) systèmes de comptes rendus obligatoires ;
b) systèmes de comptes rendus volontaires ;
c) systèmes de comptes rendus confidentiels.

Dans les systèmes de comptes rendus obligatoires, on est tenu de rendre compte de certains types d'événements ou de dangers. Cela nécessite des règlements détaillés indiquant qui doit rendre compte et de quoi il doit être rendu compte. Étant donné que les systèmes obligatoires traitent principalement de questions de «matériel (hardware)», ils ont tendance à recueillir plus d'information sur des défaillances techniques que sur d'autres aspects des activités opérationnelles. Pour aider à surmonter ce biais, les systèmes de comptes rendus volontaires visent à acquérir plus d'information sur ces autres aspects.

Dans les systèmes de comptes rendus volontaires, l'auteur du compte rendu, sans aucune obligation légale ou administrative de le faire, soumet volontairement des informations sur des événements ou des dangers. Dans ces systèmes, les agences et/ou organismes de réglementation peuvent offrir des

incitations à rendre compte. Par exemple, il peut être renoncé à des mesures d'application pour des événements dont il est rendu compte en soulignant des erreurs ou des violations non intentionnelles.

L'information dont il est rendu compte ne devrait pas être utilisée contre les auteurs de comptes rendus, ce qui signifie que ces systèmes doivent être non punitifs et doivent offrir une protection aux sources d'information, afin d'encourager la communication de cette information.

Les systèmes de comptes rendus confidentiels visent à protéger l'identité de l'auteur du compte rendu. C'est la seule façon d'assurer que les systèmes de comptes rendus volontaires soient non punitifs. La confidentialité est généralement réalisée par une dépersonnalisation, et toute information permettant d'identifier l'auteur du compte rendu est connu seulement de « dépositaires », pour permettre un suivi ou « remplir les vides » dans les événements dont il est rendu compte. Les systèmes de comptes rendus confidentiels facilitent la mise en évidence de dangers menant à l'erreur humaine, sans crainte de « justice vengeresse » ou d'atteintes à la réputation, et ils permettent une plus large acquisition d'information sur les dangers.

Tandis que les processus de base qui sous-tendent les systèmes de comptes rendus sont normalisés, les exigences de comptes rendus peuvent varier entre États et entre organisations. Il importe aussi de noter, pour assurer le succès des systèmes de comptes rendus, qu'il y a une réticence normale, de la part du personnel opérationnel, à présenter des comptes rendus. Il y a des raisons à cette réticence : représailles, auto-incrimination et atteinte à la réputation, pour ne mentionner que les trois principales.

L'éducation relative à l'importance des comptes rendus de sécurité dans les systèmes d'identification de dangers, et la protection des sources d'information de sécurité sont des stratégies essentielles pour surmonter la réticence à rendre compte et assurer un environnement de communication de comptes rendus de sécurité efficace. De bons systèmes de comptes rendus de la sécurité ont typiquement les qualités suivantes :

a) les comptes rendus sont faciles à établir ;
b) les comptes rendus n'entraîneront pas de mesures disciplinaires ;
c) les comptes rendus sont confidentiels ;
d) le retour d'information est rapide, accessible et informatif.

Les études sur la sécurité sont des analyses assez vastes, englobant de larges préoccupations relatives à la sécurité. C'est par un examen dans le contexte le plus large possible que certains problèmes de sécurité résistants peuvent être compris le mieux possible. Une organisation pourrait éprouver une préoccupation de sécurité de nature globale, qui pourrait avoir été abordée à l'échelle d'une industrie ou d'un État. Une compagnie aérienne pourrait, par exemple, enregistrer une augmentation des événements liés à l'approche et à l'atterrissage (approches instables, atterrissages profonds, atterrissages à vitesse excessive, etc.). Au niveau global, l'industrie s'est préoccupée de la fréquence et de la sévérité des accidents à l'approche et à l'atterrissage (ALA), a réalisé des études de grande ampleur, a produit de nombreuses recommandations de sécurité et a mis des mesures en application à l'échelle mondiale pour réduire ces événements pendant les phases critiques d'approche et d'atterrissage des vols. La compagnie aérienne en question peut ainsi trouver dans ces

recommandations et ces études globales des arguments convaincants pour sa propre analyse de sécurité interne. De tels arguments sont nécessaires pour réaliser des modifications à grande échelle, exigeant des données significatives, une analyse appropriée et des communications efficaces. Des arguments de sécurité fondés sur des occurrences isolées et des informations anecdotiques ne suffiraient pas. Les études de sécurité sont, par nature, plus appropriées pour s'atteler aux carences de sécurité du système que pour identifier des dangers individuels spécifiques.

Il est procédé à des examens de la sécurité lors de l'introduction et du déploiement de technologies nouvelles, de la modification ou de la mise en œuvre de procédures, ou en situations de changement structurel dans les opérations. Les examens de la sécurité sont une composante fondamentale de la gestion du changement. Ils ont un objectif clairement défini qui est lié au changement considéré. Par exemple, si un aéroport envisage de mettre en œuvre un équipement de détection à la surface de l'aéroport (ASDE), l'objectif de l'examen de la sécurité serait d'évaluer les risques de sécurité associés à cette mise en œuvre à l'aéroport XYZ en évaluant le caractère approprié et l'efficacité des activités de gestion de la sécurité relatives au projet. Les examens de la sécurité sont effectués par des groupes d'action pour la sécurité (GAS), qui s'intéressent à la performance effective des activités de gestion de la sécurité ci-après, dans le cadre des changements proposés :

a) identification des dangers et évaluation/atténuation des risques de sécurité ;
b) mesure de la sécurité ;
c) responsabilités de la direction ;
d) compétences opérationnelles du personnel ;
e) systèmes techniques ;
f) opérations anormales.

Une fois que la performance de chaque activité de gestion de la sécurité dans le cadre des changements proposés est examinée, le GAS produit une liste de préoccupations relatives à des dangers pour chaque activité, la parade/l'atténuation proposée par le cadre hiérarchique, et une évaluation du caractère approprié des atténuations et de leur efficacité pour parer aux dangers. L'atténuation sera efficace si elle gère constamment les risques de sécurité de façon à les rendre ALARP. Le GAS propose aussi une hiérarchisation des parades/atténuations, en attribuant à chaque danger une importance et un degré d'urgence. Les examens de sécurité assurent donc la performance de sécurité en périodes de changement, en apportant une feuille de route pour des changements sûrs et efficaces.

Les audits se focalisent sur l'intégrité du SGS de l'organisation et évaluent périodiquement l'état des contrôles des risques de sécurité. Comme les autres exigences, les exigences d'audit sont laissées au niveau fonctionnel, ce qui permet un large éventail de complexité, correspondant à la complexité de l'organisation. Les audits sont « externes » aux unités qui interviennent dans les activités directement liées à la fourniture de services, mais « internes » à l'organisation dans son ensemble. Ils ne sont pas destinés à être des audits approfondis des processus techniques, mais plutôt à donner une assurance des fonctions, activités et ressources de gestion de la sécurité des différentes unités. Il s'agit de

s'assurer que la structure du SGS est satisfaisante en ce qui concerne la dotation en personnel, la conformité aux procédures et instructions approuvées, les niveaux de compétence et de formation pour utiliser l'équipement et les installations et maintenir les niveaux requis de performance, etc.

Les enquêtes sur la sécurité examinent des éléments particuliers ou des procédures particulières d'une certaine opération, telles que des aspects problématiques ou des goulets d'étranglement dans les opérations quotidiennes, les perceptions et opinions du personnel opérationnel et les domaines de dissension ou de confusion. Les enquêtes de sécurité peuvent faire intervenir l'utilisation de listes de vérification, questionnaires et entrevues confidentielles informelles.

Les enquêtes étant subjectives, une vérification peut être nécessaire avant que des mesures correctives puissent être prises. Les enquêtes peuvent constituer une source peu coûteuse de renseignements significatifs concernant la sécurité.

Les investigations internes sur la sécurité incluent des occurrences ou événements dont il n'est pas exigé qu'ils fassent l'objet d'investigations ou de comptes rendus, bien que les organisations puissent, dans certains cas, mener des investigations internes indépendamment du fait que l'événement en question fait l'objet d'investigations menées par l'autorité de l'aviation civile. Des occurrences ou événements qui relèveraient d'investigations internes sur la sécurité seraient, par exemple : turbulence en vol (opérations aériennes); encombrement des fréquences (ATC) ; défaillance du matériel (maintenance) ou opérations de véhicules sur l'aire de trafic (aérodrome).

En conclusion, la contribution des diverses sources d'information sur la performance et la surveillance de la sécurité pour le SGS d'une organisation peut être résumée comme suit :

a) les comptes rendus de dangers sont une source d'information primordiale sur les dangers dans les opérations ;
b) les études sur la sécurité sont une source d'information sur les préoccupations génériques en matière de sécurité et/ou les carences systémiques de la sécurité ;
c) les examens de la sécurité sont liés à la gestion du changement et assurent la performance de sécurité dans des conditions opérationnelles changeantes ;
d) les audits s'assurent de l'intégrité des structures et processus du SGS ;
e) les enquêtes de sécurité fournissent un échantillonnage d'opinions et perceptions d'experts sur certains domaines problématiques dans les opérations quotidiennes ;
f) les investigations internes sur la sécurité portent sur des événements d'ampleur mineure dont il n'est pas exigé qu'ils fassent l'objet d'investigations.

Critères d'évaluation

• L'organisme dispose d'un processus ou d'un système qui permet la saisie de renseignements internes englobant les incidents, les accidents, les dangers et toute autre donnée pertinente au SGS.

• Le processus de compte rendu est simple, accessible et adapté à la taille de l'organisme.

• Les comptes rendus sont examinés au niveau de gestion approprié.

• Il existe un processus de rétroaction qui permet de faire savoir aux expéditeurs que leurs comptes rendus ont été reçus et de leur faire partager les résultats de l'analyse.

• Le ou les formulaires de compte rendu sont simples, normalisés et accessibles dans tout l'organisme.

• Il existe un processus permettant de s'assurer que des renseignements sont reçus de tous les domaines de l'organisme englobés par le SGS.

• Il y a un processus de surveillance et d'analyse des tendances.

• L'organisme peut compter sur un processus d'enquête et d'analyse systématiques des conditions ou des activités opérationnelles qui ont été identifiées comme étant potentiellement dangereuses.

• Les processus de collecte des données au sein de tous les domaines sensibles à la sécurité de l'entreprise permettent une analyse des questions de sécurité à la grandeur de l'entreprise.

• Des mesures correctives et préventives sont générées en réponse à l'analyse des dangers et des événements.

VII-2. Gestion du changement

Les organismes d'aviation connaissent un changement permanent dû à l'expansion, à la contraction, à des modifications dans les systèmes, équipements, programmes, produits et services existants, et à l'introduction de nouveaux équipements ou procédures. Des dangers peuvent être introduits par inadvertance dans une opération lorsqu'un changement se produit. Les pratiques de gestion de la sécurité exigent que les dangers qui sont un sous-produit du changement soient identifiés de façon systématique et proactive, et que des stratégies de gestion des risques de sécurité des conséquences de dangers soient élaborées, mises en œuvre et évaluées par la suite. Les examens de la sécurité, discutés précédemment, sont une précieuse source de renseignements et d'aide à la décision dans des circonstances de changement.

Le changement peut introduire de nouveaux dangers et avoir des incidences sur le caractère approprié ou l'efficacité des stratégies existantes d'atténuation des risques de sécurité. Les changements peuvent être externes ou internes à l'organisation. Des exemples de changements externes seraient des changements dans les exigences réglementaires ou les exigences de sûreté, ou la réorganisation du contrôle de la circulation aérienne. Des exemples de changements internes seraient des changements dans la direction, de nouveaux équipements ou de nouvelles procédures.

Un processus formel de gestion du changement devrait tenir compte des trois considérations suivantes:

a) **Criticité des systèmes et des activités.** La criticité est étroitement liée au risque de sécurité. Elle a rapport aux conséquences potentielles de l'utilisation inappropriée d'un équipement ou de l'exécution incorrecte d'une activité essentiellement par la réponse à la question, « quelle est l'importance de cet équipement/cette activité pour la sécurité des opérations du système ? » C'est une considération qui devrait intervenir au cours du processus de conception du système, mais elle devient pertinente pendant une situation de changement. Il est clair que certaines activités sont plus essentielles que d'autres pour la sécurité de la fourniture des services. Par exemple, les changements dans les activités ou les procédures relatives au retour en service d'un aéronef après un gros entretien, dans une organisation qui a mis en œuvre pour la première fois son propre service de maintenance alors qu'elle sous-traitait précédemment la maintenance à un tiers, pourraient être considérés comme plus critiques qu'un scénario semblable concernant des changements dans des activités de fourniture de repas. L'équipement et les activités d'une plus grande criticité en matière de sécurité devraient être examinés à la suite d'un changement pour s'assurer que des mesures correctives pourraient être prises pour maîtriser les risques de sécurité qui pourraient émerger ;

b) **Stabilité des systèmes et contextes opérationnels.** Les changements peuvent être le résultat d'un changement programmé tel que la croissance, les vols vers de nouvelles destinations, les changements dans le parc aérien ou dans les services sous-traités, ou d'autres changements relevant directement de l'organisation. Les changements dans le contexte opérationnel sont également importants, par exemple changements dans la situation économique ou financière, conflits du travail, changements dans le contexte politique ou réglementaire, ou changements dans le milieu physique, tels les changements cycliques dans les conditions météorologiques. Ces facteurs ne relèvent pas directement de l'organisation, mais elle doit prendre des dispositions pour y réagir. De fréquents changements dans les systèmes ou dans les contextes opérationnels exigeront que les gestionnaires actualisent l'information clé plus fréquemment que dans des situations plus stables. C'est une considération essentielle dans la gestion du changement ;

c) **Performance passée**. La performance passée de systèmes critiques est un indicateur prouvé de la performance future. C'est ici qu'entre en jeu le caractère en boucle fermée de l'assurance de la sécurité. Les analyses de tendances dans le processus d'assurance de la sécurité devraient être utilisées pour suivre au fil du temps les paramètres de performance de sécurité et factoriser cette information dans la planification des activités futures en situations de changement. De plus, lorsque des carences ont été constatées et corrigées comme résultat d'audits, d'évaluations,

d'enquêtes ou de comptes rendus passés, il est essentiel que cette information soit prise en considération pour assurer l'efficacité des mesures correctives.

Une gestion formelle du processus de changement devrait ensuite identifier les changements au sein de l'organisation qui pourraient affecter des processus, procédures, produits ou services établis. Avant de mettre en œuvre des changements, une gestion formelle du processus de changement devrait décrire les arrangements devant assurer la performance de sécurité. Ce processus a pour résultat de ramener au niveau ALARP les risques de sécurité résultant de changements dans la fourniture de services par l'organisation.

Critères d'évaluation

• L'organisation a élaboré et tient à jour un processus formel pour identifier les changements en son sein qui pourraient affecter les processus et les services établis ;

• Le processus formel pour la gestion du changement analyse les changements dans les opérations ou dans le personnel clé pour les risques de sécurité ;

• L'organisation a établi des arrangements pour s'assurer de la performance de sécurité avant la mise en œuvre de changements ;

• L'organisation a établi un processus pour éliminer ou modifier les moyens de maîtriser les risques de sécurité qui ne sont plus nécessaires du fait de changements dans l'environnement opérationnel.

VII-3. Amélioration continue du SGS

L'assurance se fonde sur le principe du cycle d'amélioration continue. À peu près de la même façon que l'assurance qualité facilite des améliorations continues dans la qualité, l'assurance de la sécurité assure la maîtrise de la performance de sécurité, y compris la conformité à la réglementation, par la vérification constante et l'amélioration du système opérationnel. Ces objectifs sont réalisés par l'emploi d'outils semblables: évaluations internes et audits indépendants (internes et externes), contrôles rigoureux des documents et surveillance continue des moyens de contrôler la sécurité et des mesures d'atténuation.

Les évaluations internes impliquent l'évaluation des activités opérationnelles de l'organisation ainsi que des fonctions spécifiques du SGS. Les évaluations menées pour répondre à cette exigence doivent être effectuées par des personnes ou des organisations qui sont fonctionnellement indépendantes du processus technique à évaluer (par exemple un service spécialisé d'assurance de la sécurité ou de la qualité ou une autre subdivision, selon les instructions de la haute direction). La fonction d'évaluation interne exige aussi l'audit et l'évaluation des fonctions de gestion de la sécurité, de définition des politiques, de gestion des risques de sécurité, d'assurance de la sécurité et de promotion de la sécurité. Ces audits rendent les gestionnaires désignés responsables de l'inventaire par le SGS de ses propres processus. Les audits internes sont un important outil à utiliser par les

gestionnaires pour obtenir les renseignements sur lesquels se fonder pour prendre des décisions et maintenir en bonne voie les activités opérationnelles. La responsabilité première pour la gestion de la sécurité réside chez les responsables d'activités techniques de l'organisation appuyant la fourniture des services. C'est ici que les dangers sont le plus directement rencontrés, que les carences dans les activités contribuent à des risques de sécurité, et que le contrôle par une supervision directe et par l'affectation de ressources peuvent atténuer les risques de sécurité en les ramenant au niveau ALARP. On pense souvent aux audits internes comme test ou « classement » des activités d'une organisation, mais ce sont des outils essentiels dans l'assurance de la sécurité, pour aider les managers/cadres responsables d'activités appuyant la fourniture de services à vérifier que, une fois que des contrôles des risques de sécurité ont été mis en œuvre, ils continuent de fonctionner et sont efficaces pour maintenir de façon continue la sécurité opérationnelle.

Les audits externes du SGS peuvent être menés par l'instance de réglementation, des partenaires de partage de code, des associations de clients ou d'autres tiers choisis par l'organisation. Ces audits n'apportent pas seulement une solide interface avec le système de supervision, mais constituent aussi un système d'assurance secondaire.

L'amélioration continue du SGS vise donc à déterminer les causes immédiates d'une performance inférieure à la normale et leurs incidences sur le fonctionnement du SGS, et à redresser les situations où intervient une performance inférieure à la normale, identifiée par des activités d'assurance de la sécurité. Réalisée sur la base d'évaluations internes et d'audits internes et externes, elle s'applique à :

a) l'évaluation proactive d'installations, d'équipement, de documents et de procédures, par exemple, par des évaluations internes ;

b) l'évaluation proactive de la performance d'une personne, pour vérifier qu'elle s'acquitte de ses responsabilités en matière de sécurité, par exemple, par des vérifications de compétence périodiques (formulaire d'évaluation/audit) ;

c) des évaluations réactives visant à vérifier l'efficacité du système pour contrôler et atténuer les risques de sécurité, par exemple, par des audits internes et externes.

En conclusion, une amélioration continue ne peut se produire que lorsque l'organisation fait preuve d'une vigilance constante concernant l'efficacité de ses opérations techniques et de ses mesures correctives. En effet, sans une surveillance constante des moyens de contrôler la sécurité et des mesures d'atténuation, il n'y a aucune façon de dire si le processus de gestion de la sécurité atteint ses objectifs. De même, il n'y a aucun moyen de mesurer si un SGS remplit efficacement son rôle.

Critères d'évaluation

• L'organisation a élaboré et tient à jour un processus formel pour identifier les causes d'une performance du SGS inférieure à la normale

• L'organisation a établi un ou des mécanismes pour déterminer les incidences sur les opérations d'une performance du SGS inférieure à la normale

• L'organisation a établi un ou des mécanismes pour éliminer ou atténuer les causes d'une

performance du SGS inférieure à la normale

• L'organisation a un processus pour l'évaluation proactive des installations, de l'équipement, de la documentation et des procédures (par le biais d'audits et d'enquêtes, etc.)

• L'organisation a un processus d'évaluation proactive de la performance d'une personne, pour vérifier qu'elle s'acquitte de ses responsabilités en matière de sécurité

VIII- Promotion de la Sécurité

VIII-1. Formation et sensibilisation

La formation et l'éducation relatives à la sécurité devraient être constituées de ce qui suit :

a) un processus documenté pour identifier les besoins en matière de formation ;

b) un processus de validation qui mesure l'efficacité de la formation ;

c) une formation initiale (sécurité générale) spécifique à l'emploi ;

d) inclusion de la familiarisation/formation initiale dans le SGS, y compris les facteurs humains et facteurs organisationnels ;

e) formation périodique à la sécurité.

Les besoins et les activités de formation devraient être documentés pour chaque domaine d'activité au sein de l'organisation. Un dossier formation devrait être établi pour chaque employé, y compris les cadres, pour aider à identifier et suivre ses besoins de formation et vérifier que le personnel a reçu la formation prévue. Les programmes de formation devraient être adaptés pour répondre aux besoins et à la complexité de l'organisation.

La formation à la sécurité au sein d'une organisation doit assurer que le personnel soit formé et compétent pour accomplir ses tâches de gestion de la sécurité. Le Manuel du SGS (MSGS) devrait spécifier des normes de formation initiale et périodique pour le personnel opérationnel, les cadres et les superviseurs, les dirigeants et le Dirigeant responsable. L'ampleur de la formation à la sécurité devrait correspondre à la responsabilité de la personne et à son implication dans le SGS. Le MSGS devrait spécifier aussi les responsabilités en matière de formation à la sécurité, notamment le contenu, la fréquence, la validation et la gestion des dossiers de formation à la sécurité.

La formation à la sécurité devrait suivre une démarche modulaire. Pour le personnel opérationnel, elle devrait porter sur les responsabilités en matière de sécurité, consistant notamment à suivre toutes les procédures d'exploitation et de sécurité, à reconnaître les dangers et à en rendre compte. Les objectifs de la formation devraient comprendre la politique de sécurité de l'organisation, ainsi que les fondamentaux et une vue d'ensemble du SGS. Le contenu devrait inclure la définition des dangers, des conséquences et des risques, le processus de gestion des risques de sécurité, y compris les rôles et les responsabilités, et le ou les systèmes de compte rendu de sécurité de l'organisation.

La formation à la sécurité pour cadres et superviseurs devrait porter sur les responsabilités de sécurité, y compris celle de promouvoir le SGS et d'engager le personnel opérationnel à rendre

compte des dangers. En plus des objectifs de formation établis pour le personnel opérationnel, ceux qui concernent les cadres et les superviseurs devraient inclure une connaissance détaillée du processus de sécurité, de l'identification des dangers, de l'évaluation et de l'atténuation des risques de sécurité, et de la gestion du changement. En plus du contenu spécifié pour le personnel opérationnel, le contenu de la formation pour les superviseurs et les cadres devrait inclure l'analyse des données de sécurité.

La formation à la sécurité pour dirigeants/cadres supérieurs devrait inclure les responsabilités en matière de sécurité, y compris le respect des exigences nationales et de celles de l'organisation en matière de sécurité, l'affectation de ressources, la réalisation d'une communication entre services en matière de sécurité et la promotion active du SGS. En plus des objectifs pour les deux précédentes catégories, la formation à la sécurité pour les dirigeants/cadres supérieurs devrait inclure l'assurance de la sécurité et la promotion de la sécurité, les rôles et les responsabilités en matière de sécurité, et l'établissement de niveaux de sécurité acceptables.

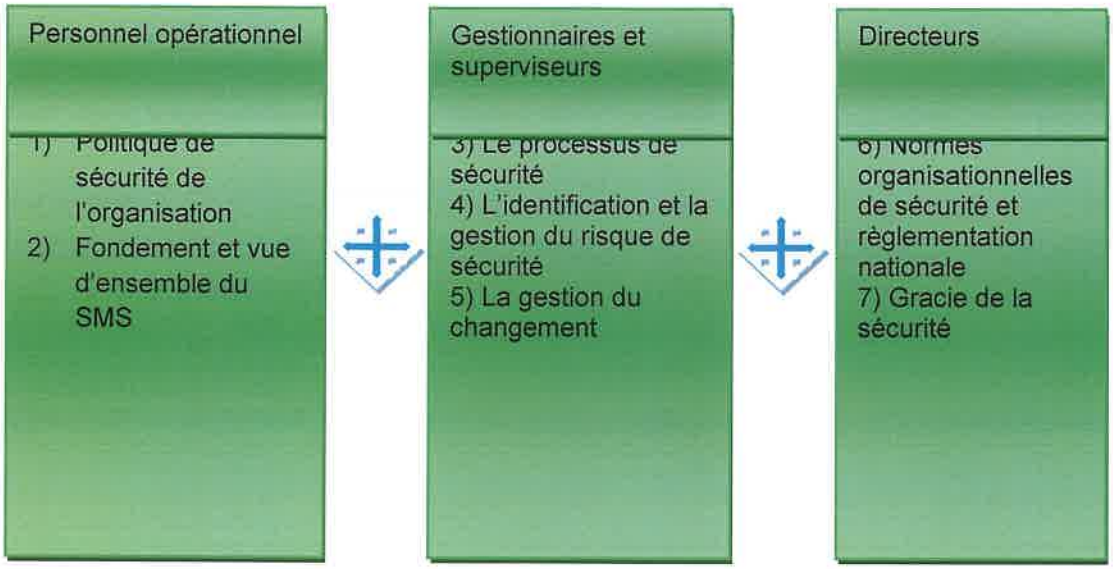

Figure 2 : Modules de formation en matière de gestion de la sécurité

En dernier lieu, la formation à la sécurité devrait inclure une formation particulière pour le Dirigeant responsable. Elle devrait être dispensée lors d'une séance de formation assez courte (qui ne devrait pas dépasser une demi-journée) et devrait lui apporter une familiarisation générale avec le SGS de l'organisation, incluant les rôles et les responsabilités relatives au SGS, la politique et les objectifs de sécurité, la gestion des risques de sécurité et l'assurance de la sécurité.

Critères d'évaluation

- Les exigences de formation sont documentées.
- Il existe un processus de validation pour mesurer l'efficacité de la formation.
- La formation comprend, le cas échéant, une formation initiale, périodique et de mise à jour.
- La formation en gestion de la sécurité de l'organisme est incorporée à la formation de familiarisation dispensée en début d'emploi.

VIII-2. Communication en matière de sécurité

L'organisation devrait communiquer à tout le personnel opérationnel les objectifs et procédures du SGS, lequel devrait être visible dans tous les aspects des opérations de l'organisation appuyant la fourniture des services. Le gestionnaire de la sécurité devrait communiquer par des bulletins et des briefings la performance du programme SGS de l'organisation. Il devrait aussi veiller à une large diffusion des enseignements tirés des enquêtes et des études de cas ou des expériences, tant à l'interne qu'en provenance d'autres organisations. La communication devrait circuler entre le gestionnaire de la sécurité et le personnel opérationnel à travers toute l'organisation. La performance de sécurité sera plus efficace si le personnel opérationnel est activement encouragé à identifier les dangers et à en rendre compte. La communication relative à la sécurité vise donc à :

a) s'assurer que tout le personnel ait pleinement connaissance du SGS ;
b) transmettre l'information critique pour la sécurité ;
c) expliquer pourquoi certaines mesures sont prises ;
d) expliquer pourquoi des procédures de sécurité sont introduites ou modifiées ;
e) transmettre l'information sur ce qui est « bon à savoir ».

Les moyens de communication peuvent inclure :

a) le manuel des systèmes de gestion de la sécurité (MSGS) ;
b) des processus et procédures de sécurité ;
c) des lettres d'information, avis et bulletins sur la sécurité ;
d) des sites web ou courriel.

Critères d'évaluation

- Des processus de communication sont en place au sein de l'organisation pour permettre un fonctionnement efficace du système de gestion de la sécurité ?
- Les processus de communication (écrite, réunions, électronique, etc.) correspondent à la taille du prestataire de services et à la portée de ses activités ;
- L'information critique pour la sécurité est établie et tenue à jour dans un média approprié qui apporte une orientation concernant les documents SGS pertinents ;
- L'information critique pour la sécurité est diffusée à travers toute l'organisation et l'efficacité des communications intéressant la sécurité est surveillée ;

• Il existe une procédure qui explique pourquoi certaines mesures de sécurité sont prises et pourquoi des procédures de sécurité sont introduites ou modifiées.

IX- Supervision de la sécurité

Après l'acceptation du SGS des fournisseurs de services de la navigation aérienne et des aérodromes, les services d'inspection ANS et AGA doivent établir et mettre en œuvre une surveillance continue de leur SGS au moins une fois l'an.

Les services d'inspection des fournisseurs de services de la navigation aérienne et des aérodromes de l'ANAC incorporent la supervision des SGS des fournisseurs de services de la navigation aérienne et des aérodromes dans leur programme annuel de surveillance continue qui incluent les mesures suivantes :

- Organiser, de concert avec les fournisseurs de services de la navigation aérienne et des aérodromes, des examens des spécifications des SGS et des éléments indicatifs connexes pour en assurer la pertinence et le bien-fondé ;
- Mesurer les performances de sécurité des SGS des fournisseurs de services de la navigation aérienne et des aérodromes par des examens des performances de sécurité convenues et s'assurer que les indicateurs de performances de sécurité (SPI), les cibles et les alertes restent pertinent aux fournisseurs de services ;
- S'assurer que les procédures d'identification des dangers et de gestion des risques de sécurité des fournisseurs de services répondent aux exigences réglementaires établies et que les mesures de contrôle des risques de sécurité sont intégrées comme il faut dans les SGS de ces fournisseurs de services