REPUBLIQUE DU CAMEROUN

Paix – Travail - Patrie

AUTORITE AERONAUTIQUE

Le Directeur Général

REPUBLIC OF CAMEROON

Peace - Work - Fatherland

CAMEROON CIVIL AVIATION AUTHORITY

The Director General

Circulaire N° 000010 /C/CCAA/DG du 17 MAI 2023

Relative à Gestion des Risques de Sécurité dans le cadre d'un système de gestion de la sécurité d'un prestataire de services aéronautiques

Version 1.0

TABLE DES MATIERES

1. Introduction 3

1.1. Objet 3

1.2. Champ d'application 3

1.3. Historique des modifications 3

1.4. Exigences 3

1.5. Documents de référence 3

2. Définitions et abréviations 4

3. Contexte 4

4. Éléments indicatifs concernant la gestion des risques de sécurité 4

4.1. Systèmes de collectes de traitements des données de sécurité 4

4.2. Détermination des dangers 17

4.3. Évaluation et atténuation des risques de sécurité 21

5. Contact 40

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

1. INTRODUCTION

La présente circulaire a pour but de fournir des éléments d'orientation (GM) pour appuyer l'établissement et l'opérationnalisation des mécanismes de gestion des risques et d'identification des dangers, qui forment l'un des piliers du SMS.

1.1. Objet

(1) La présente circulaire a pour objet d'expliciter les notions qui se rapportent à la gestion des risques de sécurité et à l'identification des dangers dans le cadre d'un SMS ; et de donner fournir quelques éléments pour aider les prestataires de services aéronautiques à rendre fonctionnels leurs mécanismes de gestion des risques.

(2) Elle couvre les points suivants :

- Détermination des dangers.
- Évaluation et atténuation des risques de sécurité.

1.2. Champ d'application

La présente circulaire s'applique à tout Prestataire de service aéronautique, ainsi que définit à l'article 2 de l'arrêté N°8/A/MINT du 10 juin 2019, basé sur le territoire camerounais.

1.3. Historique des modifications

INDICE MODIFICATION		DATE		JUSTIFICATION(S) DE LA MODIFICATION / OBSERVATIONS
Edition	**Révision**	**Issue**	**Effectivité**	
01	*00*	*11/05/2023*	*Dès signature*	*Mise en place d'éléments d'orientation en matière de SMS*

1.4. Exigences

(a) L'arrêté N°8/A/MINT du 10 juin 2019 fixant les règles de mise en œuvre des systèmes de gestion de la sécurité (SMS) par les prestataires de services aéronautiques

1.5. Documents de référence

(a) Manuel de Gestion de la Sécurité Doc 9859 - OACI, 4ième édition, 2018.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

2. DEFINITIONS ET ABREVIATIONS

(1) Les définitions suivantes sont utilisées dans la présente circulaire :

(a) **Évènement indésirable** : un évènement non souhaité au regard des services attendus ou fournis. L'évènement indésirable est une situation dangereuse à laquelle on fait face juste avant qu'elle ne dégénère en un accident.

(b) **Prestataire de services aéronautiques** : organisme de formation, exploitant d'aéronefs, organisme de maintenance d'aéronefs, prestataire de services de la circulation aérienne, exploitant d'aérodrome.

(2) Les abréviations suivantes s'appliquent aux fins de la présente circulaire :

(a) **SDCPS** : systèmes de collecte et de traitement des données de sécurité

3. CONTEXTE

(1) Cette Circulaire apporte des éléments d'orientation et des moyens acceptables pour se conformer aux exigences de l'Arrêté N°8/A/MINT du 10 juin 2019 qui régissent le composant « gestion des risques de sécurité » d'un système de gestion de la sécurité.

(2) Rappel de l'exigence : ***« Pour mettre en œuvre son système de gestion de sécurité, le prestataire de services aéronautiques met en place des mécanismes de gestion des risques de sécurité qui comprennent l'identification des dangers, l'évaluation des risques de sécurité et la mise en œuvre de mesures correctrices appropriées » - Arrêté N°8/A/MINT du 10 juin 2019, article 4.***

(3) Les caractéristiques du composant « gestion des risques de sécurité » sont donnés dans l'annexe à l'Arrêté 8 ainsi qu'il suit :

1. Gestion des risques de sécurité

1.1. Détermination des dangers.

1.2. Évaluation et atténuation des risques de sécurité.

4. ÉLEMENTS INDICATIFS CONCERNANT LA GESTION DES RISQUES DE SECURITE

Préalablement à l'identification des dangers il est nécessaire de disposer de données de sécurité fiables, et de les traiter.

4.1. Systèmes de collectes de traitements des données de sécurité

(1) Il est exigé des prestataires de services contraints de mettre en place un SMS, de mettre en place des systèmes de collecte et de traitement des

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

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. Les prestataires de services doivent 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.

(2) 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.

(3) 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.

(4) 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) 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.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

5.1.1. Sources de données de sécurité

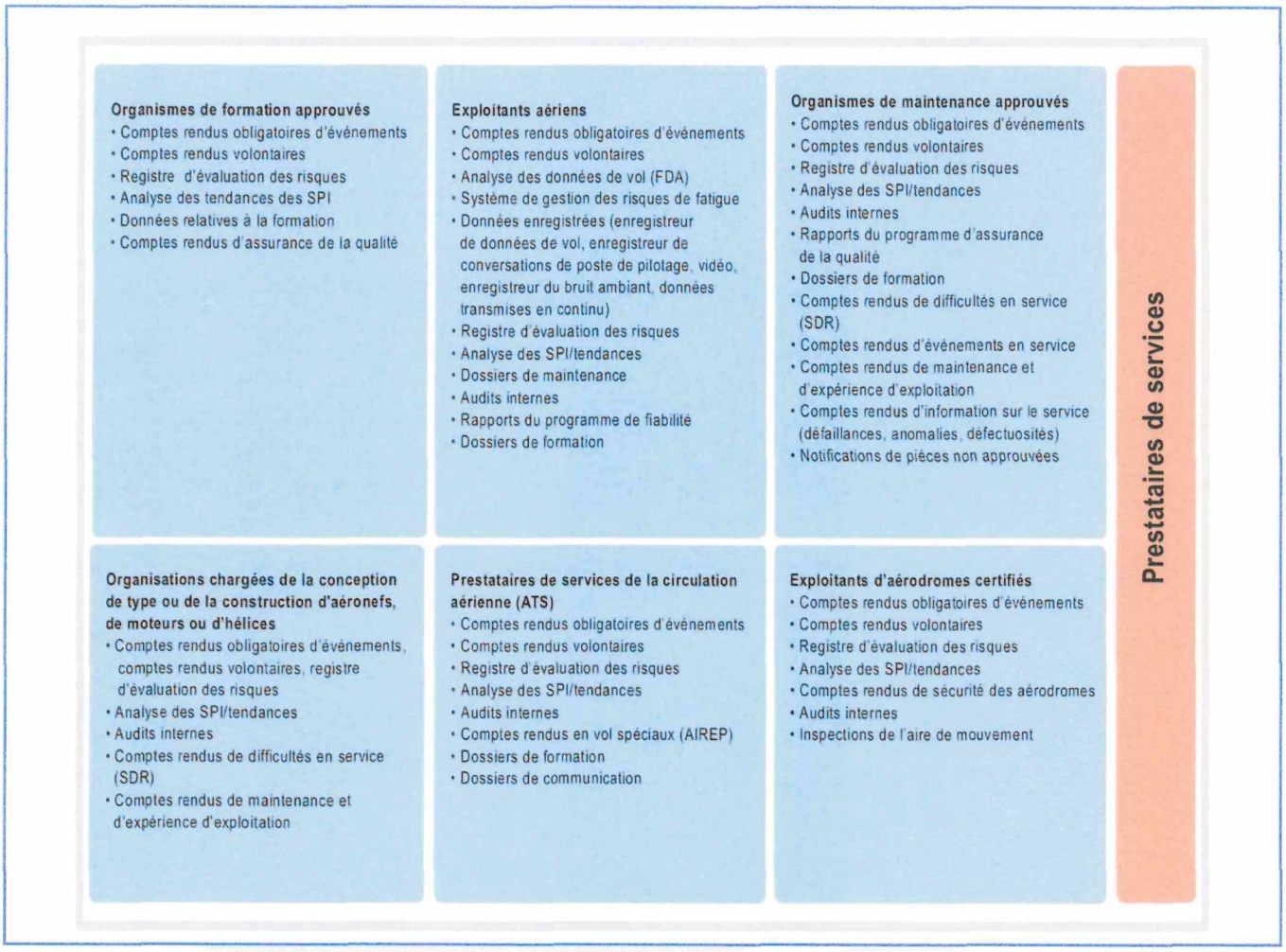


Figure 1 : Exemples de source de données pour un prestataire de service.

- ***Enquêtes sur les accidents et incidents d'aviation civile*** : un prestataire de services peut se servir des conclusions d'un accident/incident qui implique des équipements pareils que ceux dont dispose son exploitation, ou alors qui fait référence à conditions similaires à son exploitation, pour alimenter son mécanisme de gestion des risques et d'identification des dangers.
- ***Enquêtes de sécurité menées par l'autorité aéronautique ou par les prestataires de services aéronautiques.***
- ***Le système de compte rendu obligatoire en matière de sécurité*** : 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, ils devraient prévoir la saisie de certains dangers spécifiques dont

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

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.).

NB : *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 Prestataires 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'activité.*

- ***Le système de compte rendu volontaire en matière de sécurité*** : 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.
- ***Système de compte-rendu par auto-divulgation*** : Les systèmes des prestataires de services pour la collecte de données de sécurité au moyen de systèmes de compte rendu par auto-divulgation, 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.

- ***Résultats des enquêtes, audits, inspections ou évaluations*** : Les résultats d'interactions l'Autorité et le prestataire, entre les prestataires et ses sous-traitants, entre les personnels au sein de l'organisation, 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

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

sécurité tirées de ces interactions peuvent être utilisées comme preuves de l'efficacité SMS lui-même.

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.

Remarque : Les données de sécurité devraient idéalement être classées selon un langage, une codification et des définitions d'appui, afin que les données puissent être saisies et stockées sur la base de termes utiles. Les taxonomies sont alors définitions courantes qui établissent un langage/code normalisé, ce qui améliore la qualité de l'information et de la communication. Les taxonomies permettent l'analyse et facilitent le partage et l'échange d'informations.

5.1.2. Traitement des données de sécurité

(1) 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.

- **La qualité des données** : La qualité des données fait référence à des données épurées et appropriées au but recherché. La qualité des données couvre les aspects suivants :
  - ***propreté*** : 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.
  - ***pertinence*** : Les données pertinentes sont des données qui répondent aux besoins de l'organisation et représentent ses problèmes les plus importants. Une organisation devrait évaluer

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

la pertinence des données sur la base de ses besoins et de ses activités.

- ***opportunité*** : 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.
- ***précision et exactitude*** : 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.

- **Agrégation de données** : 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.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

- **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.

- **Filtrage de données** : 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

5.1.3. Gestion des données et informations de sécurité

(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 une organisation.

(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 :

i. quelles données seront collectées ;
ii. les définitions, la taxonomie et les formats des données ;
iii. comment les données seront collectées, compilées et intégrées avec les autres sources de données de sécurité et d'informations de sécurité ;
iv. 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 ;

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

v. comment les données de sécurité et les informations de sécurité seront utilisées ;
vi. comment les informations devront être partagées et échangées avec d'autres parties ;
vii. 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 ;
viii. comment la qualité sera mesurée et maintenue.

(3) En l'absence d'un processus clairement défini 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.

(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. Les personnes 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

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

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 « méga données » 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 prestataires devraient garantir que les données de sécurité, les informations de sécurité et les sources connexes bénéficient d'une protection appropriée

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

i. en quoi consistent les données ;
ii. d'où elles proviennent (source originale) ;
iii. qui les a créées ;
iv. quand elles ont été créées ;
v. qui les a utilisées ;
vi. à quelles fins elles ont été utilisées ;
vii. la fréquence de collecte ;
viii. tout traitement ou transformation.

(6) Ainsi, ces données fournissent une compréhension commune de la nature des données et 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.

5.1.4. Protection des données

(1) La protection des données de sécurité, des informations de sécurité et des sources connexes devrait être la position par défaut de toute organisation qui voudrait avoir un SMS fonctionnel. Un prestataire peut prévoir une protection effective au moyen de la politique disciplinaire, soutenues par des procédures claires et exhaustives.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

(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, vulgarisés, 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.

(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.

Un exemple d'une 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.

(4) Une manière de donner une 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, ce qui permet à ce que les informations ne sont utilisées qu'aux fins de la sécurité de l'activité du prestataire.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

(5) Si le personnel clé en charge du SMS estime que l'anonymisation des données de sécurité et des informations de sécurité ne peut prévenir efficacement l'utilisation volontaire ou permissible de données de sécurité ou d'informations de sécurité, l'anonymisation ne sera pas appropriée. C'est pourquoi les Prestataires 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.**

(6) Les exigences en matière de SMS exigent que les prestataires de services veillent à ce que les données de sécurité et les informations de sécurité ne soient pas utilisées dans des procédures disciplinaires contre des employés, du personnel d'exploitation ou des organisations, sauf si une violation est dûment constatée. Ainsi, 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. Ces processus / actions devraient être précisés dans la procédure disciplinaire de l'organisation.

(7) Cas de dérogation à la protection des données et informations de sécurité :

a. Le premier cas dans lequel la haute direction d'une organisation 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/une omission considéré(e), d'après les lois nationales, comme un cas de négligence grave, une faute intentionnelle, ou un acte criminel ».

b. Le deuxième cas dans lequel un Prestataire 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, la haute direction 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

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

disposition l'emportent sur les incidences défavorables qu'elle pourrait avoir, sur l'atmosphère de travail au sein de son organisation, sur la collecte et la disponibilité futures des données de sécurité et des informations de sécurité ».

c. Le troisième type de dérogation concerne les cas dans lesquels « après examen des données de sécurité ou des informations de sécurité », la haute direction « 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, sur l'atmosphère de travail au sein de son organisation, 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.

(8) Pour établir si un des principes régissant les dérogations s'applique dans un cas, la haute direction 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.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

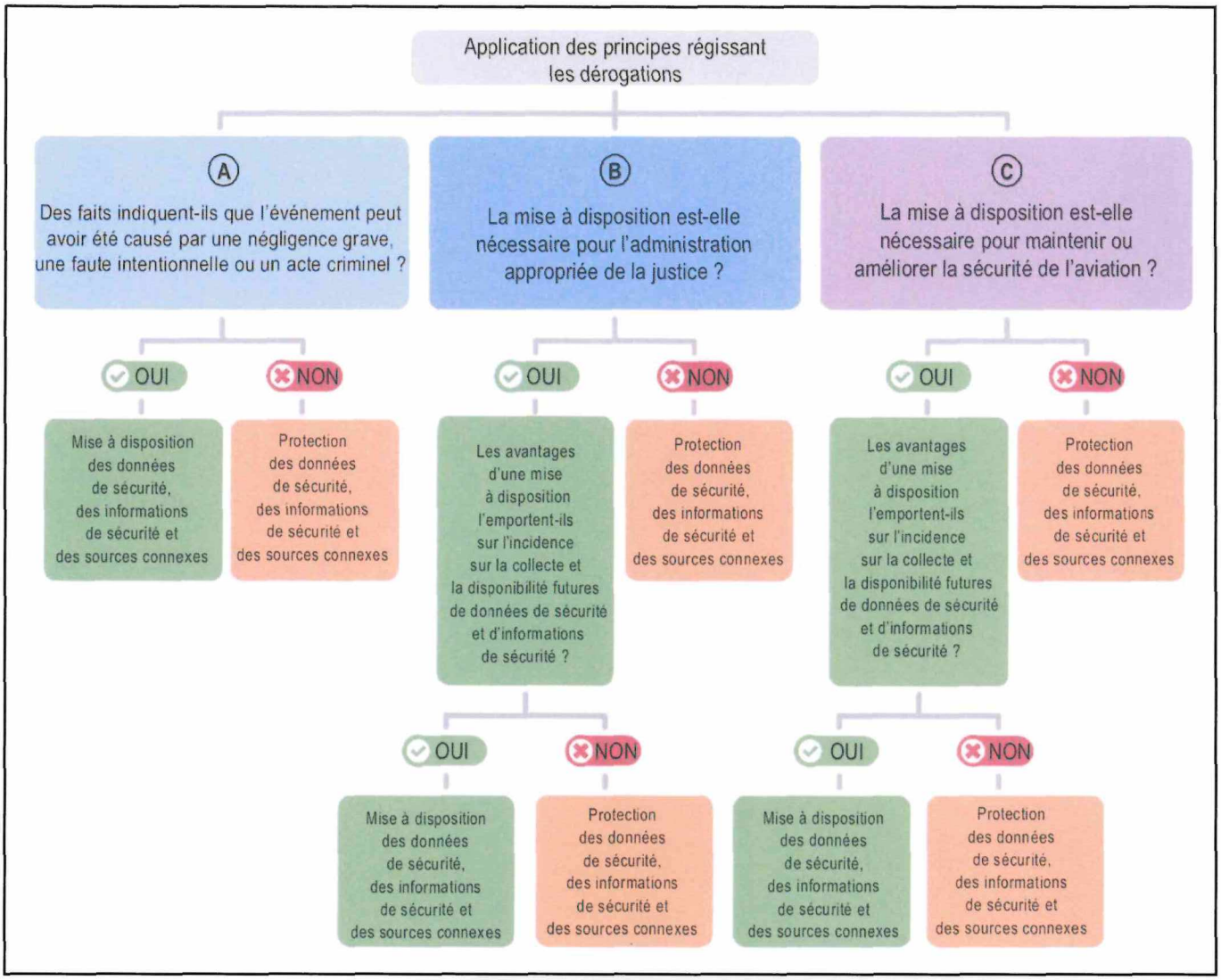


Figure 2 : Indications pour déroger à la règle sur la protection des données

5.1.4. Partage et échange des données de sécurité

(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 Prestataires agissent conformément aux principes suivants, dans le processus de partage et d'échange d'informations de sécurité :

a. le respect des principes régissant la protection de données de sécurité en vigueur dans l'État, et toutes autres obligations multilatérales et bilatérales ;
b. le partage et l'échange d'informations de sécurité n'entraînent pas de violation, par les personnels clé en charge de la gestion de la sécurité, des mécanismes pour la protection des informations de sécurité, la protection des données à caractère personnel, le

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

secret commercial (industriel), ni de violation des droits des personnes physiques et morales ;

c. les informations de sécurité partagées et échangées par un prestataire de services ne devraient pas être utilisées d'une manière qui influe négativement sur le prestataire lui-même, ses activités, ses personnels et ses partenaires ainsi qu'à d'autres fins inappropriées ;
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. Un cadre pour le partage et l'échange d'informations peut reposer sur des **accords bilatéraux** entre Prestataires de services insérés, par exemple, dans leurs protocoles d'accords ou plans de gestion des interfaces. Pour faciliter le partage et l'échange d'informations, les prestataires peuvent aussi convenir que de tels accords sont provisoirement d'application, le cas échéant, dans l'attente de leur ratification et entrée en vigueur.

(2) Les prestataires devraient promouvoir et faciliter l'établissement de réseaux pour le partage et l'échange d'informations de sécurité entre les usagers du système aéronautique.

4.2. Détermination des dangers

(1) L'identification des dangers est la première étape du processus de gestion des risques de sécurité. Elle précède une évaluation des risques de sécurité et requiert une compréhension claire des dangers et de leurs conséquences.

(2) 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.

Exemple de danger : *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*

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

pour l'exploitation, du fait de son potentiel de contribuer à une instabilité de l'aéronef. La diminution de la maîtrise pourrait provoquer un évènement tel qu'une sortie latérale de piste.

Remarque : Introduction aux notions de danger et risque de sécurité

En aviation, un danger peut être considéré comme un élément 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).

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 des risques, visant à réduire la possibilité qu'un danger aboutisse à une situation dangereuse ou évènement indésirable. L'aviation peut coexister avec des dangers pour autant que ceux-ci soient maitrisés.

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.

Le risque de sécurité, quant à lui, est l'association de la probabilité d'occurrence d'un évènement dit « indésirable », et de la gravité ou sévérité des conséquences dudit évènement sur les personnes, les équipements les infrastructures et l'environnement. Ainsi, un risque de sécurité représente le couple (probabilité, sévérité) associé à un événement d'aviation civile. On parlera donc de **« risque de sécurité associé à un évènement »**.

(3) 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 (brainstorming) 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.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

- 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.

NB : 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.

(4) Un processus d'identification des dangers standard s'articule autour des éléments suivants :

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 ;

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

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/SMS avec d'autres organisations.

(5) Il existe trois 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.

c. **Prédictive**. 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.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

	Réactive *(Analyses des évènements passés)*	Proactive *(Analyses des évènements présents)*	Prédictive *(Analyses des évènements futurs)*
But	Comprendre ce qui a mal tourné.	Comprendre ce qui ne va pas.	Comprendre ce qui pourrait mal tourner.
Quand ?	Dans le cas des incidents, incidents graves et accidents qui se sont déjà produits.	Augmentation inexpliquée/redondance d'événements de sécurité pendant les activités en cours.	Avant tout changement susceptible d'avoir un impact sur la sécurité de l'activité d'un prestataire.
Sources de données	Rapports d'analyse des incidents, rapports d'accidents, comptes rendus d'évènements de sécurité issus du système obligatoire de notification d'évènement de sécurité.	Audits, inspections, suivi / observation de l'activité, comptes rendus issus du système volontaire de notification d'évènement de sécurité.	Projections quant à l'activité, stratégie de développement de l'activité, étude de sécurité, prévisions quant à l'activité, prévisions quant au système aéronautique...

Tableau 1 : Méthodes d'identification des dangers

(6) Dans le cas d'un SMS mature, le processus d'identification des dangers (et de gestion des risques qui y sont associés) est continu car il y a fréquemment soit des incidents (*réactifs*), soit des occurrences répétées (*proactives*), soit des changements à venir (*prédictifs*).

4.3. Évaluation et atténuation des risques de sécurité

(1) Une fois les dangers identifiés, les risques associés doivent être évalués en termes de probabilité et de gravité.

(2) La probabilité doit être basée sur la fréquence de l'événement déclencheur qui pourrait conduire à l'événement indésirable, tandis que la gravité doit être basée sur les résultats de la conséquence ultime en considérant le scénario le plus probable. En outre, l'efficacité des barrières existantes (prévention et protection) doit être prise en compte.

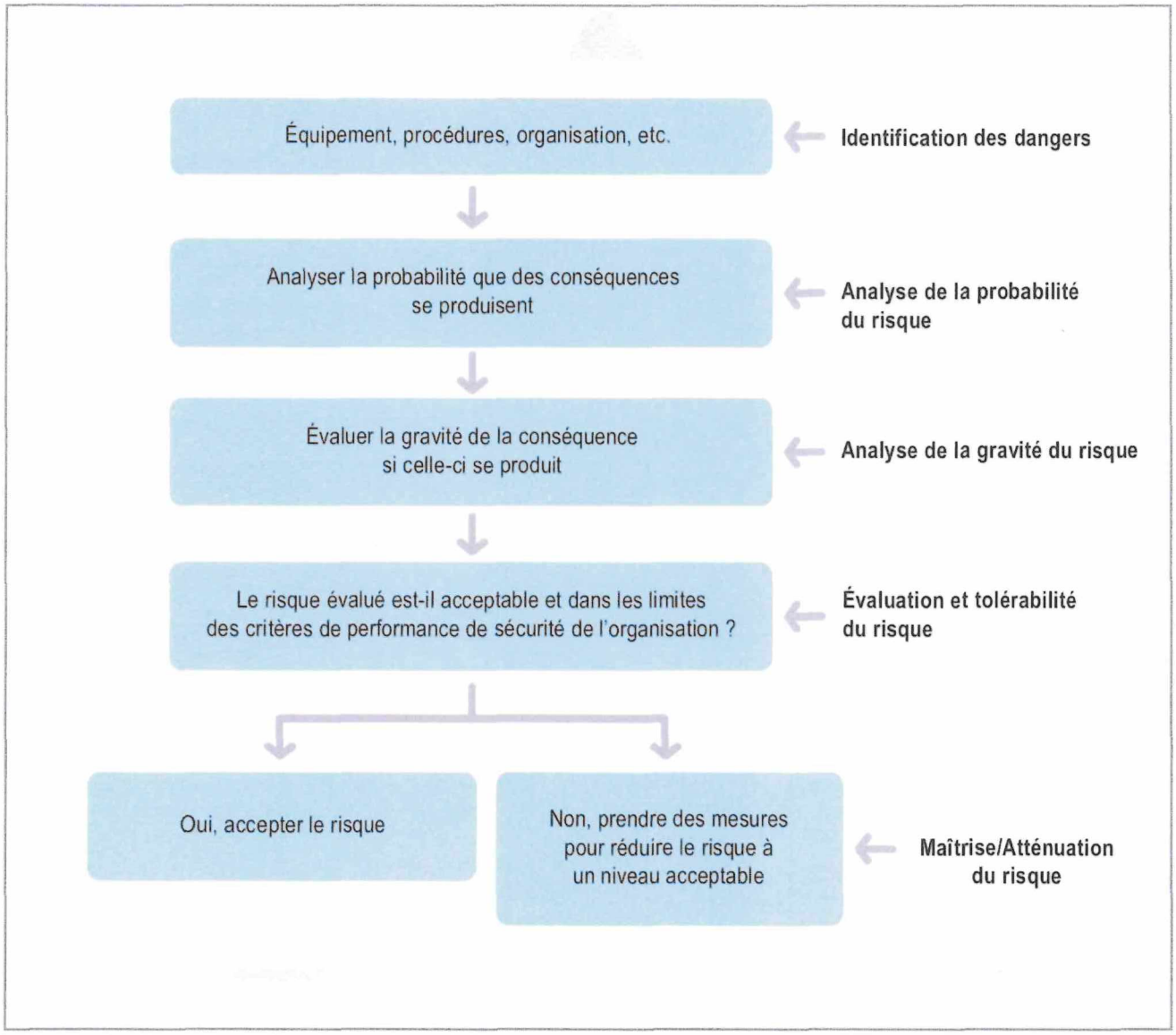
(3) L'évaluation des risques suppose que des échelles graduées pour mesurer à la fois la probabilité et la gravité doivent être définies en fonction du contexte quant à l'activité du prestataire de service.

(4) La définition des degrés de probabilité peut être basée sur des critères

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

qualitatifs ou quantitatifs pertinents pour les services fournis (*Ex : période de temps, nombre de mouvements, ...*). Et la définition des degrés de gravité peut être basée sur les différents aspects impactés (personnes, biens, environnement, réputation).

(5) La combinaison des deux échelles graduées conduit à la matrice de tolérance des risques.



Processus d'identification des dangers et de gestion des risques

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

5.3.1. Probabilité des risques de sécurité

(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 ; autrement dit, la probabilité correspond à la fréquence d'occurrence d'une situation dangereuse ou d'un évènement indésirable.

NB : *On entend par « évènement indésirable (EI) » un évènement non souhaité au regard des services attendus ou fournis. L'évènement indésirable est une situation dangereuse à laquelle on fait face juste avant qu'elle ne dégénère en un accident.*

(2) Généralement, le travail d'évaluation et d'atténuation du risque associé se fait par rapport aux EI, d'où 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 :

i. Existe-t-il un historique d'occurrences similaires à celle qui est en cours d'examen ou s'agit-il d'un cas isolé ?
ii. D'autres équipements ou éléments du même type pourraient-ils présenter des défectuosités semblables ?
iii. Au sein du personnel, quel est le nombre de personnes qui appliquent les procédures considérées ou qui y sont soumises ?
iv. 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 ?

(3) Assez généralement les organisations mettent en place un canevas, une classification qui leur permet de définir méthodiquement la probabilité d'un risque de sécurité. Cette méthode qualitative se résume dans le tableau ci-dessous

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

Probabilité	Signification	Valeur
Fréquent	Susceptible de se produire de nombreuses fois. *(s'est produit fréquemment)*	**5**
Occasionnel	Peut se produire de temps en temps, de façon sporadique. *(ne s'est pas produit fréquemment.)*	**4**
Faible	Peu susceptible de se produire, mais possible. *(s'est produit rarement)*	**3**
Improbable	Ne devrait pas se produire mais reste néanmoins possible. *(on n'a pas connaissance que cela se soit produit)*	**2**
Extrêmement rare	Il est presque inconcevable que l'événement se produise.	**1**

Tableau 2 : Exple d'échelle de probabilité

NB : 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.*

(4) Un autre exemple d'échelle de probabilité basée sur des critères quantitatifs est présenté dans la table ci-dessous :

Probabilité	Critère de classification
Fréquent	Au moins une fois tous les 1.000 mouvements d'aéronefs.
Occasionnel	Au moins une fois tous les 10.000 mouvements d'aéronefs.
Faible	Au moins une fois tous les 100.000 mouvements d'aéronefs.
Improbable	Au moins une fois tous les 1.000.000 mouvements d'aéronefs.
Extrêmement rare	Moins d'une fois sur 1.000.000 de mouvements d'aéronefs

Tableau 3 : Exple d'échelle de probabilité.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

5.3.2. Gravité/sévérité d'un risque de sécurité

(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 d'un évènement indésirable, ou comme résultat du danger identifié. La classification de la gravité devrait tenir compte des éléments suivants :

- **les pertes de vies humaines ou les blessures graves qui surviendraient** du fait :
  - de la présence dans l'aéronef ;
  - du contact direct avec une partie quelconque de l'aéronef, y compris avec des parties qui s'en sont détachées ; ou
  - de l'exposition directe au souffle des réacteurs ; et

- **les dommages** :
  - **dommages ou défaillances structurelles subis par l'aéronef** :
    - qui altèrent ses caractéristiques de résistance structurelle, de performance ou de vol ;
    - qui normalement devraient nécessiter une réparation importante ou le remplacement de l'élément endommagé ;

  - **dommages subis par les ATS ou les équipements d'un aérodrome** :
    - qui ont une incidence négative sur la gestion de la séparation des aéronefs ; ou
    - qui ont une incidence négative sur la capacité d'atterrissage.

  - **dommages subis par des infrastructures tierces, au sol, qui ne sont ni l'aéronef, ni les infrastructures côté piste de l'aérodrome**.

(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 ci-dessous 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.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

Tableau 4 : Exple d'échelle de gravité.

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 puissent accomplir leurs tâches de façon exacte ou complète (perturbation à long terme des services fournis). • Blessures graves • Importants dommages aux équipements	**B**
Majeur	• 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 (perturbation à court terme des services fournis). • Dommages sur l'aéronef ou autres équipements qui pourraient être rapidement réparés • Personnes blessées (Blessure nécessitant un traitement médical)	**C**
Mineur	• Nuisance • Limites de fonctionnement • Recours à des procédures d'urgence (perturbation mineure des services fournis). • Éventuelles perturbations des opérations ayant des conséquences sur les coûts • Dommages mineurs à un aéronef ne permettant pas de suspendre son exploitation.	**D**
Négligeable	• Peu de conséquences • Pas de dégradation des marges de sécurité • Irrégularité d'exploitation	**E**

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

Tableau 5 : Un autre exemple d'échelle de gravité.

Gravité	Signification par rapport à l'impact sur l'environnement	Signification par rapport à l'impact sur la réputation du Prestataire
Catastrophique	Contamination à long terme (radioactivité, eaux souterraines empoisonnées, écosystème détruit).	Impact, de telle sorte que la communauté cesse de recourir aux services du prestataire sur une longue période de temps.
Dangereux	Contamination à court terme (écosystème touché mais non détruit).	Impact, de telle sorte que la communauté réduit son recours aux services fournis par le prestataire pendant une période prolongée.
Majeur	Contamination maîtrisée (Ex : un déversement de carburant sur une plateforme).	Impact, de telle sorte que la communauté réduit son recours aux services fournis par le prestataire pendant une courte période de temps.
Mineur	Impact mineur sur l'environnement	Impact, tel que la communauté remet en question la fiabilité des services fournis par le Prestataire.
Négligeable	Pas d'impact sur l'environnement	Pas d'impact sur la réputation.

5.3.3. Indice de risque de sécurité et notion de « tolérabilité » du risque

(1) L'indice de risque de sécurité est obtenu à partir des résultats des scores de probabilité et de gravité. Dans l'exemple ci-dessous, on a choisi d'utiliser un code alphanumérique pour matérialiser cet indice. Les combinaisons gravité/probabilité respectives sont présentées dans une matrice d'évaluation des risques de sécurité telle que celle présentée ci-après. Cette matrice sert à déterminer la tolérabilité du risque de sécurité, et à classer l'évènement indésirable ou situation dangereuse. En d'autres termes, cette matrice sera pour une organisation un outil pour « accepter » un risque de sécurité, ou définir un niveau de risque qui déclenchera ou non des actions d'atténuation.

Si nous prenons, par exemple, un événement pour lequel on voudrait évaluer le risque de sécurité associé et dont la probabilité d'occurrence a été évaluée comme Occasionnelle (4), et les conséquences considérées comme Dangereuses (B) en matière de gravité, on obtient un indice de risque de sécurité de (4B).

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

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 rare	1	1A	1B	1C	1D	1E

Tableau 6 : Évaluation de l'indice de risque de sécurité.

(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 ou encore d'acception pour un prestataire de service. Le Tableau ci-dessous présente **un exemple de tableau 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.

Tableau 7 : Table d'acceptation d'un risque de sécurité.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

Dans l'exemple précédent, l'indice de risque de sécurité a été évalué en tant que 4B. Ce qui relève de la catégorie « intolérable » selon le tableau de tolérabilité ci-avant. Dans ce cas, l'indice de risque de sécurité de la conséquence est classé « inacceptable ». L'organisation devrait donc prendre des mesures de maîtrise des risques adaptées à la complexité de son activité afin de réduire :

i. **l'exposition de l'organisation au danger** particulier, c'est-à-dire réduire la composante de probabilité du risque à un niveau acceptable ;
ii. **la gravité des conséquences liées au danger**, c'est-à-dire réduire la composante de gravité du risque à un niveau acceptable ; ou
iii. **à la fois la gravité et la probabilité**, de façon à ce que le risque soit géré à un niveau acceptable.

(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 est/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.

5.3.4. Évaluation des risques liés aux facteurs humains

(1) La prise en compte des facteurs humains revêt une importance particulière en gestion des risques de sécurité, car les humains peuvent être à la fois une source de risques de sécurité et une solution à ces risques en :

i. contribuant à un accident ou à un incident par une performance variable due aux limites humaines ;
ii. anticipant et en prenant des mesures appropriées pour éviter une situation dangereuse ;
iii. résolvant des problèmes, prenant des décisions et prenant des mesures pour atténuer les risques.

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.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

(2) La gestion des risques 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 :

i. 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 ;
ii. les conséquences de la variabilité de la performance humaine différeront selon la tâche effectuée et selon le contexte.

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.

5.3.5. Classification des évènements

(1) L'analyse du niveau de risque associé à un évènement de sécurité permet aussi de classer cet évènement selon sa gravité. Classer les évènements permet à une organisation de mieux structurer ses analyses de sécurité, et donne la possibilité d'être méthodique dans le traitement des données de sécurité, ainsi que dans la conduite à tenir pour résoudre les préoccupations de sécurité.

(2) Il est important qu'une méthodologie de classification soit définie au sein d'une organisation, et communiquée auprès de tous les personnels susceptibles de l'utiliser. Cela permettra d'harmoniser l'analyse des données de sécurité, et de rendre plus objective les analyses.

(3) Un exemple de méthodologie de classification est celle d'Eurocontrol, présentée dans le tableau qui suit :

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

Catégorie d'évènement	Signification	Valeur
Accident	Cf. Définition OACI.	
Incident grave	Incident impliquant des circonstances indiquant une forte probabilité d'accident et lié à l'exploitation d'un aéronef qui, dans le cas d'un aéronef avec équipage, se produit entre le moment où une personne monte à bord de l'aéronef dans l'intention d'effectuer un vol et le moment où toutes ces personnes ont débarqué, ou dans le cas d'un aéronef sans équipage, se produit entre le moment où l'aéronef est prêt à se déplacer dans l'intention d'effectuer un vol et le moment où il s'immobilise à la fin du vol et où le système de propulsion primaire est arrêté. *Note 1 - La différence entre un accident et un incident grave réside uniquement dans le résultat.* *Note 2 - Des exemples d'incidents graves figurent dans l'appendice C de l'annexe 13 de l'OACI.*	**A**
Incident Majeur	Un incident au cours duquel : • La sécurité a pu être compromise, soit en raison d'une quasi-collision entre des aéronefs, avec le sol ou des obstacles (c'est-à-dire que les marges de sécurité n'ont pas été respectées, ce qui n'est pas le résultat d'une instruction ATC). • L'évaluation de l'incident à l'aide d'un processus de classification des risques a permis d'identifier que cet incident aurait pu dégénérer en une situation plus grave.	**B**
Incident significatif	Un incident au cours duquel : • Un accident, un incident grave ou majeur aurait pu se produire si le risque n'avait pas été géré dans les marges de sécurité (une ou plusieurs barrières de sécurité restantes). Ou, • si un autre aéronef ou véhicule s'était trouvé à proximité pendant l'incident.	**C**
Incident	Un événement, autre qu'un accident, lié à l'exploitation d'un aéronef, qui affecte ou pourrait affecter la sécurité de l'exploitation. ***N.B**. Les types d'incidents qui intéressent principalement l'Organisation de l'aviation civile internationale pour les études de prévention des accidents sont énumérés dans l'appendice C de l'annexe 13 de l'OACI.*	**D**
Occurrence sans effet sur la sécurité	Un événement pouvant être lié à la sécurité (ne répondant pas aux exigences de déclaration). Eurocontrol : Un incident qui n'a pas d'importance pour la sécurité. N.B. Ceci semble être en contradiction avec la définition de l'OACI d'un incident : Un événement, autre qu'un accident, lié à l'exploitation d'un aéronef qui affecte ou pourrait affecter la sécurité de l'exploitation. Un événement éventuellement lié à la sécurité ne répondant pas aux exigences de notification. Cela peut être, par exemple, le résultat d'un déclassement de l'incident après examen.	**E**

Tableau 8 : Exple de méthode de classification des évènements de sécurité.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

5.3.5. Stratégies d'atténuation des risques de sécurité

Atténuation = mise en place de mesures visant à traiter le danger potentiel, ou à réduire la probabilité ou la gravité du risque.

(1) L'atténuation des risques est basée sur les défenses ou barrières de sécurité (éléments présents dans un système pour le protéger d'un risque de sécurité) qui sont soit des contrôles préventifs, soit des mesures de récupération mis en place pour empêcher l'occurrence d'un événement dangereux ou ses conséquences.

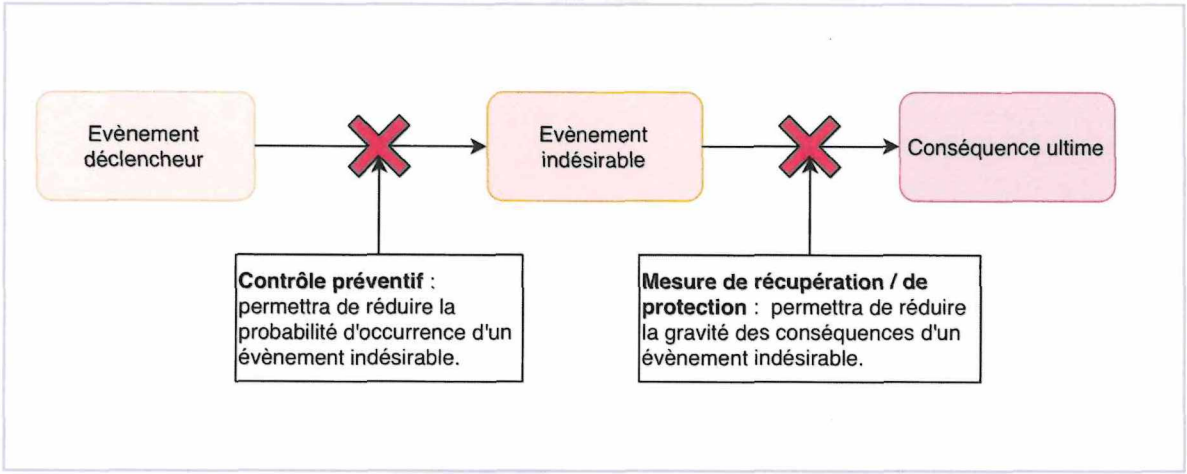


Figure 3 : Principe d'atténuation du risque de sécurité.

(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 :

i. ***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.

ii. ***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.

iii. ***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.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

(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 pratique sur le terrain 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 de risque plus efficace et plus complète.

(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 :

i. ***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.

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

iii. ***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.

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

v. ***Applicabilité***. Mesure dans laquelle le respect de nouvelles règles, de nouveaux règlements ou de nouvelles procédures d'exploitation peut être suivi.

vi. ***Durabilité***. Mesure dans laquelle l'atténuation sera durable et efficace.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

vii. ***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.

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

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

(5) Une fois que les mesures d'atténuation des risques ont été définies, il convient de réévaluer les risques en tenant virtuellement compte des mesures définies, et de vérifier dans la matrice si la situation s'est améliorée en termes de probabilité et/ou de gravité. Si l'on peut s'attendre à une amélioration grâce à ces mesures, il faut alors les mettre en œuvre - en tenant compte de l'équilibre entre le coût et le temps - et en assurer le suivi.

NB : *Il faudrait toujours avoir à l'esprit qu'une gestion efficace des risques cherche à maximiser les avantages de l'acceptation d'un risque (une réduction du temps et des coûts), tout en minimisant le risque lui-même. Autrement dit : atteindre le niveau de risque le plus bas qu'il soit raisonnablement possible d'atteindre (ALARP).*

(6) Les mesures d'atténuation et de maîtrise des risques de sécurité devront être vérifiées, et donc 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.

5.3.6. Implications de la sous-traitance dans la gestion de la sécurité

Pour que le management des risques soit efficace pour tous les prestataires de services, il est important de définir clairement les responsabilités quant à l'identification des dangers et la gestion des risques de sécurité associés pour toute la chaîne de services au sein du système, et ce sans lacunes ni chevauchements.

Lorsqu'un prestataire de services contraint à l'exigence du SMS passe un contrat avec une organisation non soumise à cette exigence, les dangers et les risques de sécurité potentiellement introduits par l'entrepreneur sont traités par le SMS du prestataire de services. Cela confère au prestataire de services des responsabilités supplémentaires pour s'assurer qu'il est bien informé des risques pour la sécurité induits par les activités de son (ses) entrepreneur (s). Les

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

activités sous-traitées doivent toutes faire partie du champ d'application de l'agrément/Certificat du Prestataire, et sont réalisées par une autre organisation, soit elle-même certifiée ou autorisée à réaliser ces activités, soit, si elle n'est pas certifiée ou autorisée, travaillant sous l'agrément/certificat et la surveillance du Prestataire.

	Activité sous contrat - soumise à la certification ; et - le Prestataire de services certifié pour cette activité	Activité sous contrat - soumise à la certification ; et - le Prestataire de service NON certifié pour cette activité
Organisation externe contractuelle certifiée pour fournir l'activité.	Un Prestataire effectue un contrôle de conformité du sous-traitant (l'organisation externe contractuelle) et doit au moins vérifier que le certificat couvre effectivement les activités contractuelles, et qu'il est valide.	Un prestataire de services effectue un contrôle de conformité du sous-traitant (l'organisation externe contractuelle) et doit au moins vérifier que le certificat couvre effectivement les activités sous contrat, et qu'il est valide.
Organisation externe sous contrat NON certifiée pour fournir l'activité.	L'organisation externe sous contrat travaille sous la supervision du prestataire de services.	L'activité ne peut pas être sous-traitée à l'organisation externe.

Tableau 9 : Responsabilité du Prestataire en cas de sous-traitance.

5.3.7. Documentation de la gestion des risques la sécurité

(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 (comme le registre de danger Cf : GM relatif à la politique et aux objectifs de sécurité). 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) 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'algorithme d'aide à la prise de décision en matière de risque de sécurité est présenté ci-dessous, il pourrait être considéré comme un processus type de gestion des risques de sécurité :

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

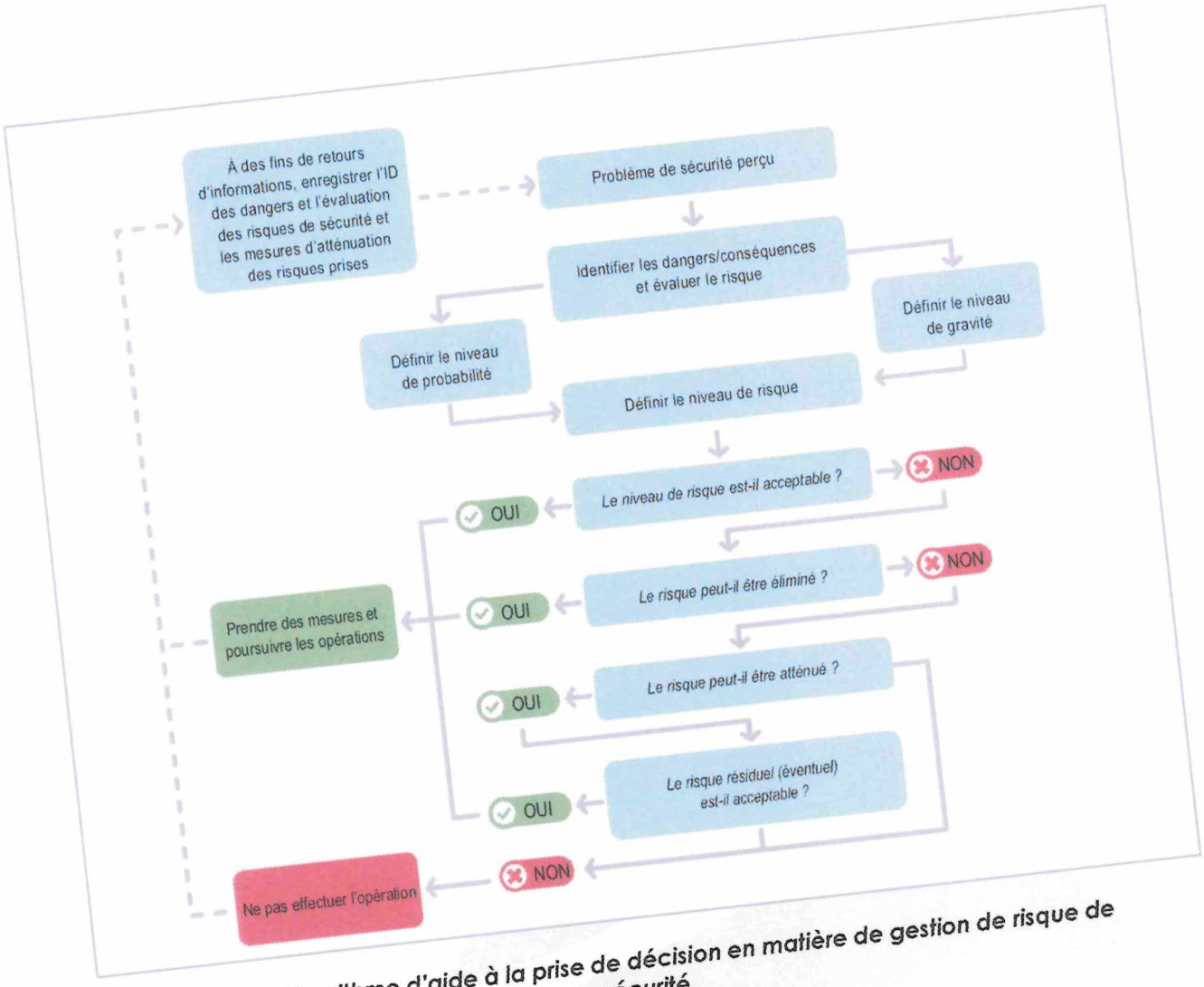


Figure 4 : Algorithme d'aide à la prise de décision en matière de gestion de risque de sécurité

Remarque : Analyse « coûts vs 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 décisions stratégiques 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.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92
Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

(3) Un autre document fard qui permette de documenter une étude de risque est la cartographie des risques (*Cf : GM relatif à la politique et aux objectifs de sécurité*). L'une des méthodes les plus généralement utilisées pour établir une cartographie de risque est la méthode du **« diagramme papillon » ou « bow tie »**.

(4) La méthode Bow tie est une méthode d'évaluation des risques qui peut être utilisée pour analyser et démontrer les relations de causalité dans les scénarios à haut risque.

(5) Un diagramme Bow tie présente deux avantages principaux. Tout d'abord, il donne un résumé visuel de tous les scénarios d'accident plausibles qui pourraient exister autour d'un certain événement indésirable. Deuxièmement, en identifiant les mesures de contrôle / barrière, le Bowtie montre ce qu'une entreprise fait pour maîtriser le risque associé à un évènement indésirable.

(6) Le diagramme papillon représente les scénarios dans une séquence ordonnée dans le temps, de gauche à droite.

- Le danger et l'événement indésirable étudiés se trouvent au centre du diagramme.
- Les évènements déclencheurs sont placés à gauche de l'événement indésirable.
- Les conséquences ultimes sont placées à droite de l'événement indésirable.

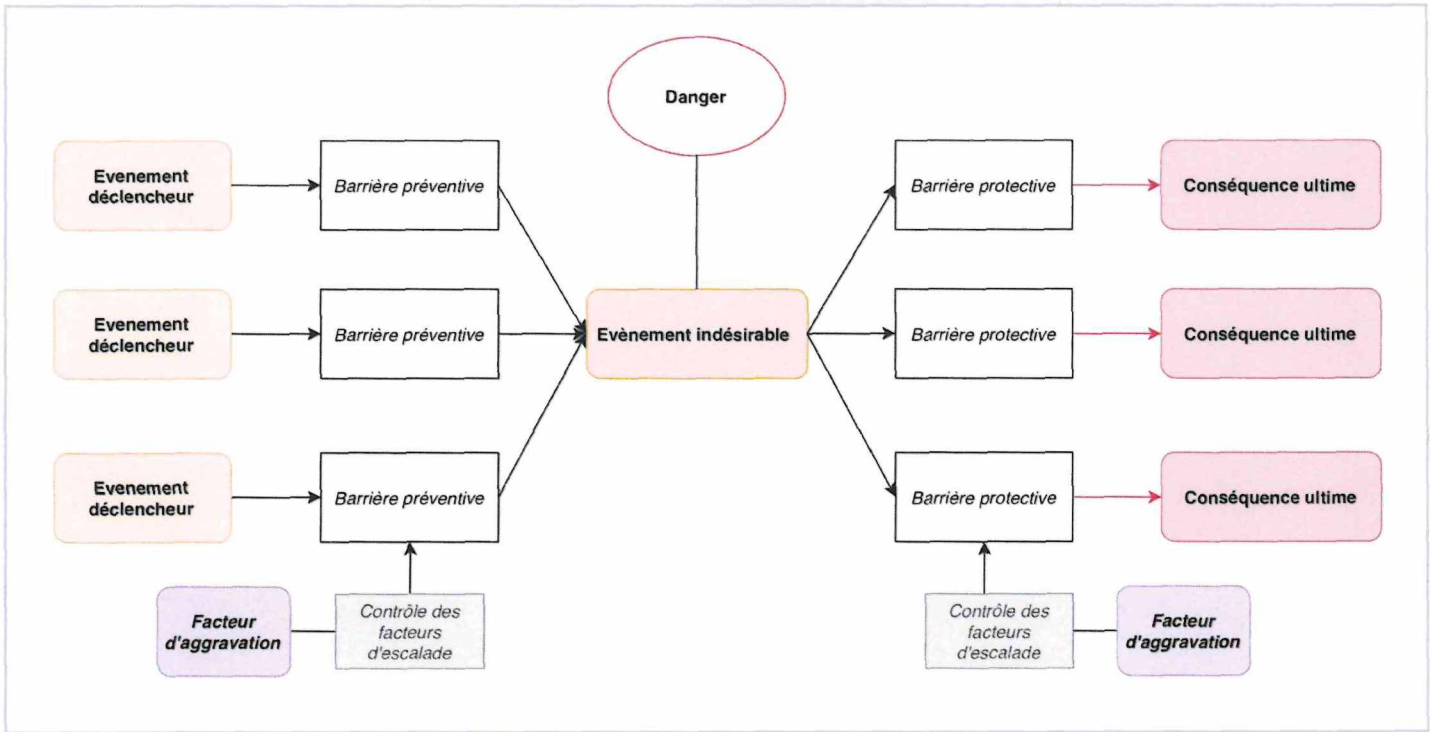
(7) Il doit y avoir une relation logique de cause à effet entre un évènement déclencheur et l'événement indésirable, afin que tout lecteur soit en mesure de comprendre le lien, sur la base de la description de l'évènement déclencheur. Les questions à poser pour saisir la relation entre chaque concept et l'événement indésirable sont présentées ci-dessous.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

Élément du diagramme	Question à poser pour structurer un diagramme papillon
Danger	Un danger se rapporte-t-il à l'évènement indésirable qu'on analyse ?
Évènement indésirable	Que se passe-t-il lorsque l'évènement déclencheur n'est pas maîtrisé ?
Évènement déclencheur	Quelles sont les circonstances qui ont provoqué, ou révéler le potentiel dangereux d'un objet, ou élément inhérent au système ?
Conséquence ultime	Si l'évènement indésirable avait dégénéré jusqu'à produire un incident plus grave, voire un accident, quels auraient été l'issue et les scénarios les plus crédibles ?
Barrière préventive	Qu'est-ce qui pourrait empêcher l'évènement indésirable de produire ?
Barrière de protection	Comment peut-on empêcher l'évènement indésirable de s'aggraver et conduire à un accident ?
Facteur d'aggravation	Qu'est-ce qui pourrait entraver le fonctionnement efficace des barrières de sécurité en place.
Contrôle des facteurs d'escalade.	Comment peut-on garantir l'efficacité d'une barrière de sécurité ?

Tableau 10 : Concepts du diagramme papillon.

Le diagramme papillon se présente comme il suit :



ÅFigure 5 : Diagramme papillon.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

Exemple d'analyse réalisée à l'aide d'un diagramme papillon :

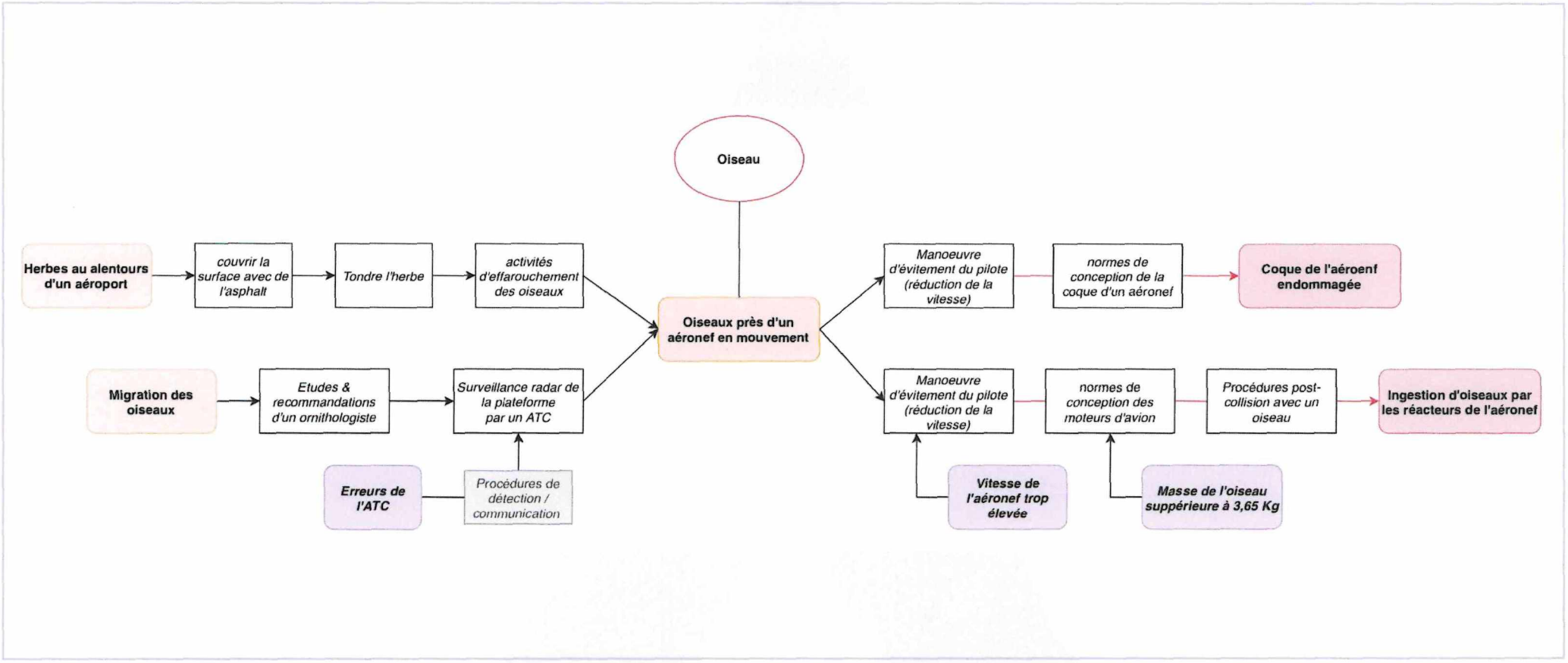


Figure 6 : d'analyse réalisée à l'aide d'un diagramme papillon.

B.P./P.O.Box : 6998 Yaoundé - Tél./Phone : +237 222 30 30 90 / 222 30 26 92 Fax : +237 222 30 33 62 - Email: contact@ccaa.aero - Site web: http://www.ccaa.aero/

5. CONTACT

(1) Pour de plus amples renseignements, veuillez contacter :

dsa@ccaa.aero

(2) Toute proposition de modification de la présente circulaire est bienvenue et peut être soumise à l'adresse électronique ci-dessus.

Yaoundé, le 17 MAI 2023

Le Directeur Général,

Paule ASSOUMOU KOKI

B.P./P.O. Box : 6008 Yaoundé Tél./Phone : +237 222 30 30 00 / 222 30 26 02 Fax : +237 222 30 33 62 Email: contact@ccaa.aero Site web: http://www.ccaa.aero/