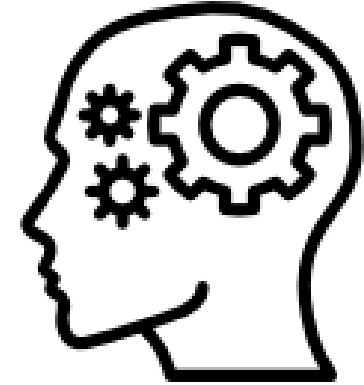


Projet UE-Afrique sur la sécurité aérienne (EU-ASA) Soutenir la mise en œuvre du PNS

Module 3

Votre sécurité est notre mission.

Le rôle des données de sécurité et des informations sur la sécurité



Note importante concernant la version française

A19
amdt. 2

- Les textes de la Lettre aux Etats 2023/18 contenus dans cette présentation ont été traduits par les service de traduction de l'Union Européenne.
- De ce fait, des différences peuvent exister dans les textes inclus dans cette présentation et la Lettre aux Etats, sans pour autant que ceci amène à des différences au niveau de l'énoncé.
- Seule la Lettre aux Etats doit être utilisée comme source officielle concernant les changements proposés.



Données de sécurité

Source : Annexe 19 de l'OACI, 1^{er} amendement

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

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

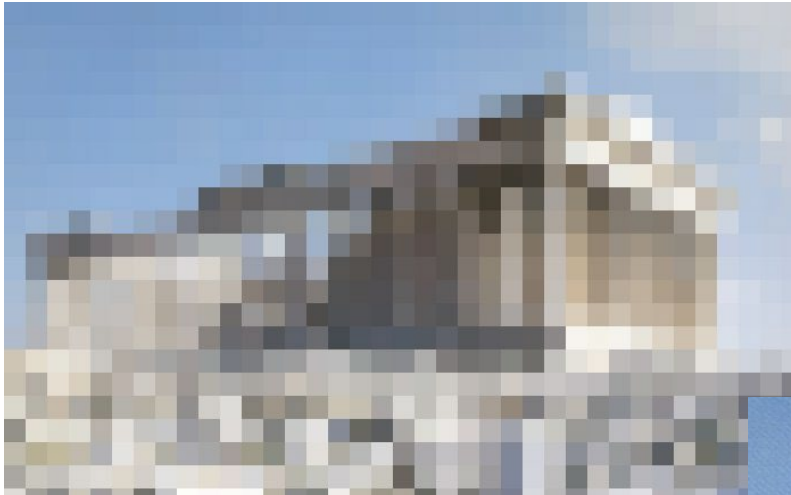
- a) les enquêtes sur les accidents ou les incidents;
- b) les comptes rendus de sécurité (obligatoires/volontaires);
- c) les comptes rendus de maintien de la navigabilité;
- d) le suivi des performances opérationnelles;
- e) les inspections, audits, enquêtes; ou
- f) les études et analyses de sécurité.



Données de sécurité traitées, organisées ou analysées dans un contexte donné de manière à les rendre utiles à la gestion de la sécurité.



Données de sécurité & information.....



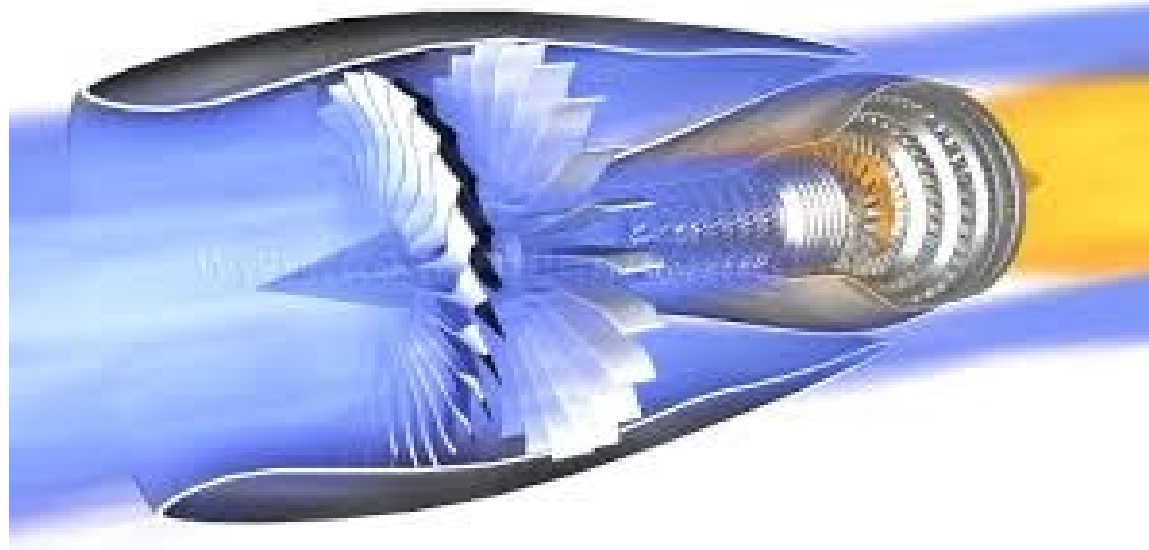
Données de sécurité

Informations de sécurité



Le «moteur» du PNS: la gestion des risques de sécurité

Carburant :
données et informations
sur les dangers et les
risques



Poussée :
prise de décision
fondée sur les
risques pour
améliorer le niveau
de sécurité et
l'efficacité

Huile (catalyseur):
Culture de sécurité positive pour la sensibilisation aux risques, la
prise de décision fondée sur les risques et pour assurer la
disponibilité continue des données et de l'information sur la
sécurité.

Annexe 19 Chapitre 5 - Contenu

5.1. Systèmes de collecte et de traitement des données de sécurité (SDCPS)

5.2. Analyse des données de sécurité et de l'information sur la sécurité

5.3. Protection des données de sécurité et des informations de sécurité

5.4. Partage et échange d'informations sur la sécurité

Annexe 19 Normes 5.1.2 & 5.1.3

Deux types de systèmes de compte rendu doivent être mis en œuvre

OBLIGATOIRE

VOLONTAIRE

Événements susceptibles de présenter un risque important pour la sécurité aérienne

Détails des événements qui peuvent ne pas être saisis dans le système de déclaration obligatoire

Autres informations relatives à la sécurité perçues comme un danger réel ou potentiel pour la sécurité aérienne

Les informations provenant des comptes rendus volontaires et obligatoires peuvent être intégrées dans un système unique (base de données).

Annexe 19 Normes 5.3.1 & 5.3.2

5.3 Protection des données et des renseignements sur la sécurité

5.3.1 Les États assureront la protection des données de sécurité saisies dans les **systèmes de compte rendu volontaires en matière de sécurité, celle des informations de sécurité provenant de ces systèmes et celle des sources connexes**, conformément aux dispositions de l'Appendice 3.

Note. — Les sources comprennent les personnes et les organisations.

5.3.2 Recommandation.— Il est recommandé que les États étendent la protection visée au point 5.3.1 aux données de sécurité saisies dans les **systèmes de compte rendu obligatoires en matière de sécurité, aux informations de sécurité provenant de ces systèmes et aux sources connexes**.

Note 1. — Un environnement dans lequel les employés et le personnel d'exploitation peuvent avoir confiance qu'ils ne seront pas sanctionnés pour des actions ou omissions qui corresponedent à leur expérience est fondamental pour la communication des comptes rendus en matière de sécurité.

Annexe 19 Normes 5.3.1 & 5.3.2

Protection des données de sécurité et des informations de sécurité

La recommandation d'étendre les protections aux systèmes de comptes rendus de sécurité obligatoires a été proposée à l'OACI. Compte tenu des lois existantes qui l'empêchent pour certains États, il n'est pas prévu d'élever le 5.3.2 à une norme.

Qu'entend-on exactement par protection?



Protection des données de sécurité et des informations de sécurité

Signification de la protection

Prendre les mesures nécessaires pour assurer la confidentialité voulue des détails des événements signalés à l'État ou stockés dans la base de données nationale.

Les données à caractère personnel (noms et adresse des personnes physiques) ne sont mises à la disposition des personnes autres que celles désignées pour évaluer de manière indépendante les comptes rendus d'événements originaux que lorsque cela est absolument nécessaire pour enquêter sur des événements en vue d'améliorer la sécurité aérienne.

Traitement des données à caractère personnel uniquement dans la mesure nécessaire au maintien ou à l'amélioration de la sécurité aérienne.

Il n'est pas nécessaire d'anonymiser complètement les rapports collectés, mais des mesures doivent être prises pour garantir la confidentialité appropriée des détails des événements contenus dans la base de données.

Protection des données de sécurité et des informations de sécurité

Utilisation appropriée des informations tirées des comptes rendus d'événements

Les informations tirées des comptes rendus d'événements ne sont utilisées qu'aux fins pour lesquelles elles ont été collectées.

S'abstenir d'intenter des poursuites pour des infractions non préméditées ou involontaires à la loi qui vous sont signalées uniquement parce qu'elles ont été signalées (comptes rendus obligatoires ou volontaires), À MOINS QU'UNE EXCEPTION NE S'APPLIQUE.

Ne pas mettre à disposition ou ne pas utiliser pas les informations sur les événements afin d'attribuer un blâme ou une responsabilité, À MOINS QU'UNE EXCEPTION NE S'APPLIQUE.

Ne pas mettre à disposition ou utiliser les informations sur les événements à d'autres fins que le maintien ou l'amélioration de la sécurité aérienne.

Exceptions au principe de protection

Norme 3 de l'appendice 3 de l'annexe de l'OACI



- Des exceptions à la protection des données de sécurité, des informations de sécurité et des sources connexes ne sont accordées que lorsque l'autorité compétente:
 - a) détermine qu'il existe des faits et des circonstances indiquant raisonnablement que l'événement peut avoir été causé par un acte ou une omission considéré, **négligence grave, faute intentionnelle ou activité criminelle;**
 - b) après avoir examiné les données de sécurité ou les informations de sécurité, détermine que leur **divulcation est nécessaire à la bonne administration de la justice;** ou
 - c) après avoir examiné les données de sécurité ou les renseignements sur la sécurité, détermine que leur **diffusion est nécessaire au maintien ou à l'amélioration de la sécurité.**

- Dans les cas visés aux points b) et c), l'État doit déterminer que les avantages de la dissémination l'emportent sur l'incidence négative qu'une telle dissémination est susceptible d'avoir sur la collecte et la disponibilité futures de données et d'informations sur la sécurité.

Comment la protection des données est réglementée en Europe

- En Europe, le règlement (UE) no 376/2014 «règlement sur les rapports d'événements» exige le même niveau de protection pour les comptes rendus / signalements obligatoires et volontaires.
- Le règlement (UE) no 376/2014 exige également:
 - Que chaque État Membre désigne un organisme indépendant chargé de la mise en œuvre des principes de la culture juste. Le personnel de l'aviation peut signaler à cet organisme les infractions présumées aux règles.
 - Que chaque organisation adopte des règles décrivant la manière dont les principes de la «culture juste» sont garantis et mis en œuvre au sein de l'organisation, après consultation des représentants du personnel.

Comment la protection des données est-elle réglementée dans votre État?

(MOR.../... VOR)



ANALYSE DES DONNEES & INFORMATIONS DE SECURITE DANS LE CADRE DU PROGRAMME NATIONAL DE SECURITE :

CAS DE LA CAMEROON CIVIL AVIATION AUTHORITY



Titre

COLLECTE, ANALYSE, PROTECTION, PARTAGE ET ÉCHANGE
DE DONNÉES DE SÉCURITÉ ET D'INFORMATIONS SUR LA
SÉCURITÉ



Nouveau titre

DÉVELOPPEMENT DE L'INTELLIGENCE EN MATIÈRE DE
SÉCURITÉ

Nouvelle Recommandation 5.1.1: Il est recommandé que les États établissent une **stratégie** pour le développement de l'intelligence de sécurité qui soutienne la gestion de la sécurité et la prise de décision.



De nouvelles orientations relatives à la stratégie de développement de l'intelligence de sécurité figurent dans le Manuel du Renseignement de Sécurité (Safety Intelligence Manual - doc. 10159 – Publication en 2025).

Justification: La recommandation souligne l'importance de **développer l'intelligence de sécurité en tant que capacité opérationnelle** et la nécessité d'un engagement organisationnel pour faire des progrès dans ce domaine. Le terme stratégie est utilisé pour exprimer l'importance du leadership organisationnel dans l'établissement des objectifs, la définition des actions et l'assurance que les ressources appropriées sont disponibles pour les mettre en œuvre.

Chapitre 5 – Principales modifications proposées avec SL 23/18

A19
amdt. 2

La Norme 5.1.1 est modifiée , désormais 5.2.1: Les États mettront en place ~~des systèmes~~ **un système de collecte et de traitement des données de sécurité (SDCPS) composé d'une série de processus et de schémas intégrés** pour saisir, stocker, agréger, **traiter** et permettre l'analyse des données de sécurité et des informations sur la sécurité.

Note 1 supprimée - SDCPS fait référence aux systèmes de traitement et de déclaration, aux bases de données de sécurité, aux systèmes d'échange d'informations et aux informations enregistrées, y compris, mais sans s'y limiter.

Justification:

Un SDCPS est élaboré à l'aide d'une série de processus intégrés définis comme une série d'activités visant à atteindre un objectif spécifique et de systèmes d'échange de données et d'informations sur la sécurité.

Un SDCPS constitue la base de l'analyse de la sécurité, qui est un catalyseur essentiel pour soutenir le développement et la maturité continue de la capacité d'une organisation en matière de renseignement de sécurité.

Chapitre 5 – Principales modifications proposées avec SL 23/18

Norm 5.1.2 Supprimée: ~~Les États mettront en place un système de compte rendu obligatoire en matière la sécurité qui inclut le compte rendu des incidents.~~

Justification: *Les États n'ont pas besoin d'établir un nouveau système de déclaration obligatoire, mais plutôt de relier les dispositions de déclaration sectorielles contenues dans d'autres annexes, PANS et documents d'orientation au SDCPS qu'ils peuvent utiliser pour soutenir les activités de gestion de la sécurité.*

A19
amdt. 2

Chapitre 5 – Principales modifications proposées avec SL 23/18

A19
amdt. 2

Nouvelle Norme 5.2.2 - Les États veilleront à ce que le SDCPS soit fondé sur des méthodes **proactives et réactives** de collecte de données et d'informations sur la sécurité.

Nouvelle Note - Un SDCPS peut inclure des contributions de l'État, de l'industrie et de sources publiques.

Justification: *L'approche réactive est la méthode la plus couramment utilisée pour la collecte de données dans le système aéronautique actuel. Il est considéré que des méthodes proactives de collecte de données doivent être utilisées pour établir et améliorer l'efficacité d'un SDCPS. La note d'appui vise à maintenir la notion de sources d'intrants.*

Nouvelle Norme 5.2.3 - Les États devront veiller à ce que les données de sécurité et les informations de sécurité recueillies au moyen de systèmes de compte rendu obligatoire de la sécurité soient intégrées dans le SDCPS.



Nouvelle Note 1 - Les systèmes obligatoires de compte rendu de sécurité comprennent la déclaration des dangers et des lacunes en matière de sécurité.

Nouvelle Note 2 - Le SDCPS comprend des systèmes de compte rendu de sécurité obligatoires établis par l'État conformément aux dispositions sectorielles contenues dans d'autres Annexes, des procédures pour les services de navigation aérienne (PANS) et des documents d'orientation à l'appui. En outre, l'Annexe 13 contient des informations sur la notification des données relatives aux accidents/incidents (ADREP). Des exemples de systèmes de compte rendu de sécurité obligatoires figurent dans le Manuel de l'Intelligence sur la Sécurité (ICAO Safety Intelligence Manual - doc. 10159).

Chapitre 5 – Principales modifications proposées avec SL 23/18

A19
amdt. 2

Justification (nouvelle note 1):

La note 1 à l'appui vise à souligner l'importance de signaler les dangers, tels que

- les **rapports de fatigue** requis à l'Annexe 6 — Exploitation d'aéronefs, Partie I — Transport aérien commercial international — Avions,
- les **rapports d'incapacité en vol requis** à l'annexe 1 — Licences du personnel, ainsi que
- les **manquements en matière de sécurité constatés dans le GASP** (doc. 10004) et la feuille de route mondiale pour la sécurité aérienne (GASR - doc. 10161),

dans le cadre des comptes rendus de sécurité obligatoires, en plus des accidents et des événements liés à la sécurité.



Recommandation 5.1.4 supprimée – ~~Il est recommandé que les autorités nationales responsables de la mise en œuvre du PNS aient accès aux SDCPS visés au § 5.1.1 aux fins de leurs responsabilités en matière de sécurité, en conformité avec les principes énoncés à l'appendice 3.~~

Nouvelle norme 5.2.5 - Les autorités de l'État responsables de la mise en œuvre du PNS **devront contribuer et** avoir accès aux données de sécurité et aux informations de sécurité dans le SDCPS pour appuyer leurs responsabilités en matière de sécurité.

Justification: *Il est proposé de mettre à niveau cette pratique recommandée afin de tenir compte du fait que la contribution et l'accès aux données et à l'information sur la sécurité sont considérés comme essentiels à l'établissement d'un SDCPS. Cette proposition de mise à niveau souligne également l'importance de la collaboration, de la coordination et de la communication entre les autorités de l'État chargées de la mise en œuvre du PNS.*

Recommandation 5.1.5 supprimée – ~~Il est recommandé que les bases de données de sécurité utilisent une taxonomie normalisée de façon à faciliter le partage et l'échange de renseignements sur la sécurité.~~

Nouvelle norme 5.2.6 - Les États **devront** utiliser une taxonomie pour les comptes rendus sur la sécurité qui est alignée sur les taxonomies normalisées et qui facilite:

- (a) l'identification des dangers au niveau du système d'aviation civile de l'État, comme indiqué au point 3.3.4;
- (b) une comparaison cohérente des données de sécurité et des informations sur la sécurité; et
- (c) le partage et l'échange d'informations sur la sécurité, comme indiqué au point 5.5.

Note modifiée - ~~Les États sont encouragés à utiliser un système compatible avec l'ADREP. De plus amples informations sur l'ADREP figurent à l'annexe 13, chapitre 7.~~

Des orientations relatives aux taxonomies normalisées, y compris, mais sans s'y limiter, la taxonomie ADREP, figurent dans le Manuel de l'Intelligence sur la Sécurité (ICAO Safety Intelligence Manual - doc. 10159).

Justification:

La recommandation a été revalorisée pour tenir compte de l'importance d'utiliser des taxonomies normalisées pour les rapports sur la sécurité au sein d'un État. Leur utilisation est importante pour la comparaison cohérente des données de sécurité et des informations sur la sécurité, le partage et l'échange d'informations sur la sécurité, en particulier entre plusieurs langues et systèmes.

Ceci assure également l'uniformité et la qualité de l'information sur la sécurité pour appuyer l'élaboration de l'intelligence sur la sécurité utilisée pour la prise de décisions.

Un avantage supplémentaire des taxonomies standardisées est leur capacité à soutenir le développement, l'application et la maintenance de méthodes d'analyse avancées et de technologies d'apprentissage automatique.

Nouvelle Recommandation 5.2.7 – Il est recommandé que les États mettent en place un **moyen de gouvernance** des données et des informations sur la sécurité.



Nouvelle Note - Des orientations supplémentaires sur la gouvernance des données de sécurité figurent dans le Manuel de l'Intelligence sur la Sécurité (ICAO Safety Intelligence Manual - doc. 10159).

Justification - S'aligner sur le nouveau 5.2.1 et souligner l'importance des données de sécurité et de la gouvernance de l'information sur la sécurité pour appuyer l'élaboration de l'intelligence sur la sécurité par les États.

La gouvernance des données est le fondement d'une stratégie sur les données de sécurité. Les données de sécurité, à leur tour, sont importantes pour la gestion des risques de sécurité et doivent être gérées correctement pour assurer la cohérence et la valeur analytique.

La gouvernance des données de sécurité et des informations sur la sécurité est une pratique recommandée pour alléger toute charge perçue par les États. Il convient également de noter que certains États doivent encore améliorer leur compréhension de la gestion des données, de ses besoins et de son importance.

Analyse des données de sécurité et des informations sur la sécurité

Norme 5.2.1 amendée ~~États mettront en place et tiendront à jour un processus d'analyse des données de sécurité et des informations relatives à la sécurité provenant du SDCPS et des bases de données de sécurité associées.~~

Désormais incluse comme Norme 5.3.1 Les États mettront en place et tiendront à jour **des processus** d'analyse des données de sécurité et des informations sur la sécurité provenant du SDCPS.

Les processus comprennent une variété de méthodes d'analyse pour soutenir l'identification:

- (a) les indicateurs de performance en matière de sécurité, comme indiqué au point 3.4.2.1;
- (b) les dangers au niveau du système de l'aviation civile de l'État, tels que mentionnés au point 3.3.4, qui pourraient autrement ne pas être identifiés par les différents prestataires de services; et
- (c) les pratiques existantes et les stratégies opérationnelles qui ont donné des résultats positifs en matière de sécurité.

Notes 1/2/3 supprimées

Chapitre 5 – Principales modifications proposées avec SL 23/18

A19
amdt. 2

Analyse des données de sécurité et des informations sur la sécurité

Justification: *L'objectif de l'analyse de sécurité devrait viser à présenter la situation en matière de sécurité de manière à permettre aux décideurs de prendre des décisions fondées sur des données. L'analyse des données de sécurité et de l'information sur la sécurité peut être effectuée de plusieurs façons, afin de fournir une compréhension plus précise de la situation globale et d'identifier les relations, les connexions, les modèles et les tendances. La portée de la norme existante et les notes à l'appui suggèrent que le processus d'analyse se limite à l'analyse des dangers, dont la portée est trop étroite compte tenu de l'objectif du sous-chapitre 5.3.*

Le changement proposé de «processus (singulier)» en «processus (pluriel)» dans la version renumérotée 5.3.1 souligne qu'un seul processus n'est pas suffisant pour traiter les différentes méthodes que les États peuvent utiliser pour l'analyse.

Chapitre 5 – Principales modifications proposées avec SL 23/18

A19
amdt. 2

Partage et échange d'informations sur la sécurité

Norme 5.4.2 amendée ~~Les Etats encourageront l'établissement de réseaux pour le partage ou l'échange des informations de sécurité entre les usagers du système aéronautique et faciliteront le partage et l'échange des informations de sécurité, sauf indication contraire dans le droit national.~~

Désormais incluse comme 5.5.2 Les États faciliteront la mise en place de moyens permettant de partager en temps utile des informations sur la sécurité afin de promouvoir la collaboration au sein de la communauté aéronautique, à condition que les mesures appropriées soient prises pour garantir que les informations sur la sécurité ne soient utilisées que pour maintenir et améliorer la sécurité.

Nouvelle Note - Les moyens de partager ou d'échanger en temps utile des informations sur la sécurité peuvent comprendre des ententes, des partenariats, des équipes de sécurité collaboratives, des forums et des plateformes numériques/physiques.



Justification: Remplacer «promouvoir» par «faciliter» renforce la responsabilité de l'État dans la création d'un environnement propice au partage et à l'échange d'informations en matière de sécurité.

Le terme «réseaux» fait généralement référence à des plateformes limitées telles que les forums et les réunions de groupe.

Afin de clarifier le champ d'application du partage et de l'échange, le terme «réseau» est remplacé par «moyens» et la nouvelle note est introduite.

Chapitre 5 – Principales modifications proposées avec SL23/18

Partage et échange d'informations sur la sécurité

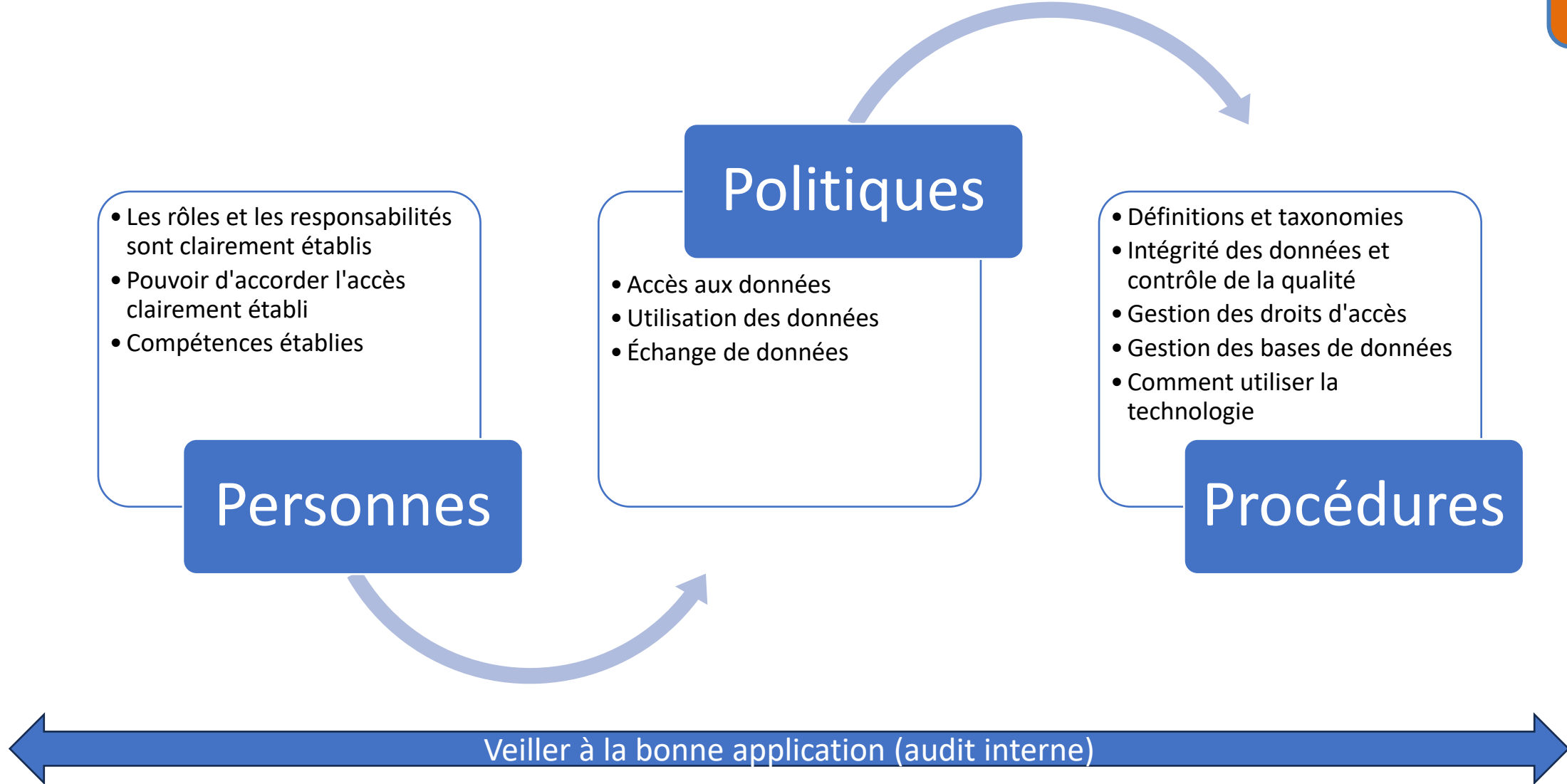
Nouvelle Recommandation 5.5.3 Il est recommandé que les États promeuvent le partage et l'échange d'informations pertinentes sur la sécurité et d'intelligence de sécurité entre les prestataires de services, à condition que les mesures appropriées soient prises pour faire en sorte que les informations de sécurité et l'intelligence de sécurité ne soient utilisées que pour maintenir et améliorer la sécurité.



Justification: *Reconnaissant que le partage et l'échange d'information pertinente sur la sécurité et de l'intelligence de la sécurité entre les prestataires de services ne peuvent être imposés, la promotion de ces activités est présentée comme une recommandation. Une mise en garde sur les conditions de protection est ajoutée afin de s'aligner sur les dispositions du point 5.4.*

C'est quoi la gouvernance des données?

A19
amdt. 2



Modifications les plus importantes proposées avec SL 23/18

- Nouveau chapitre intitulé «DÉVELOPPEMENT DE L'INTELLIGENCE EN MATIÈRE DE SÉCURITÉ »
- Nouvelle section 5.1 'General' – Sections 5.1-5.4 -> Sections 5.2 – 5.5
- Nouvelles recommandations proposées:
 - 5.1.1 établir une **stratégie pour l'élaboration de l'intelligence sur la sécurité** qui appuie la gestion de la sécurité et la prise de décisions.
 - 5.2.7 établir un **moyen de gouvernance des données et de l'information sur la sécurité.**
 - 5.5.3 **promouvoir le partage et l'échange d'informations pertinentes sur la sécurité et de l'intelligence sur la sécurité entre les prestataires de services**, à condition que les mesures appropriées soient prises pour garantir que les informations sur la sécurité et les renseignements sur la sécurité ne sont utilisées que pour maintenir et améliorer la sécurité.

Modifications les plus importantes proposées avec SL 23/18

→ Nouvelles normes:

- 5.2.2 Les États veilleront à ce que le SDCPS soit fondé sur des méthodes **proactives et réactives** de collecte de données et d'informations sur la sécurité.
- 5.2.3 Les États veilleront à ce que les données de sécurité et les informations relatives à la sécurité recueillies au moyen de systèmes de compte rendu obligatoire de la sécurité soient **intégrées dans le SDCPS**.

Modifications les plus importantes proposées avec SL 23/18

→ Recommandations mises à niveau vers le niveau norme:

- 5.2.5 Les autorités de l'État responsables de la mise en œuvre du PNS **devront contribuer et** avoir accès aux données de sécurité et aux informations sur la sécurité dans le SDCPS à l'appui de leurs responsabilités en matière de sécurité.
- 5.2.6 Les États **utiliseront une taxonomie** pour l'établissement des rapports sur la sécurité qui est alignée sur les taxonomies normalisées et qui facilite la
 - (a) l'identification des dangers au niveau du système d'aviation civile de l'État, comme indiqué au point 3.3.4;
 - (b) une comparaison cohérente des données de sécurité et des informations relatives à la sécurité; et
 - (c) le partage et l'échange d'informations en matière de sécurité, comme indiqué au point 5.5.

Modifications les plus importantes proposées avec SL 23/18

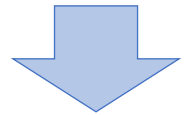
→ Clarifications fournies:

- SDCPS se compose d'une série de **processus et de systèmes intégrés**
- SDCPS basé sur des méthodes **proactives** et **réactives** de collecte de données et d'informations de sécurité
- Les dangers et les lacunes en matière de sécurité doivent également être signalés!

Thèmes pour les questions de protocole SSPIA SDA de l'OACI

- Collecte de données de sécurité & Systèmes de traitement (SDCPS)
- Système de compte rendu obligatoire (MOR)
- Système de compte rendu volontaire (VOR)
- Protection des données de sécurité
- Base de données sur la sécurité (base de données nationale)
- Garantir l'accès des autorités publiques aux données
- Capacité d'analyse de la sécurité & compétences
- Identification des dangers et évaluation des risques pour la sécurité
- Prendre des mesures à la suite de l'évaluation des risques -> PNSA
- Une culture juste

Règlement
(UE) 376/2014



va plus loin que
l'Annexe 19

Systèmes de collecte et de traitement des données de sécurité

SSP.SDA.01	Le niveau «Présent» signifie que:
Quels systèmes de collecte et de traitement des données de sécurité (SDCPS) l'État a-t-il mis en place pour soutenir l'analyse des données de sécurité au niveau de l'État?	• Un mécanisme est en place pour assurer la collecte, le traitement et l'analyse des données de sécurité au niveau de l'État. • Les sources de données et d'informations sur la sécurité comprennent les données et informations provenant des enquêtes sur les accidents et les incidents, des systèmes de comptes rendus d'événements obligatoires et d'autres sources, y compris les comptes rendus volontaires. • Il existe un mécanisme au niveau des États pour assurer la catégorisation des données de sécurité et une taxonomie convenue au niveau des États, avec des définitions à l'appui.

→ Les données de sécurité ne se limitent pas aux comptes rendus d'événements. Selon l'annexe 19, les «données de sécurité» sont un ensemble défini de faits ou de valeurs de sécurité collectés auprès de diverses sources liées à l'aviation, qui sont utilisés pour maintenir ou améliorer la sécurité.

Comptes rendus volontaires

SSP.SDA.02	Le niveau «Présent» signifie que:
Comment et dans quelle mesure l'État a-t-il établi et mis en œuvre un système de comptes rendus volontaires au niveau de l'État pour faciliter la collecte de données et d'informations sur la sécurité qui pourraient ne pas être saisies par les systèmes de compte rendu obligatoire de la sécurité?	• Il existe un système de comptes rendus volontaires. • Le système de comptes rendus volontaires est utilisé -> veiller à ce qu'une distinction puisse être faite entre les comptes rendus obligatoires et les comptes rendus volontaires! • Le système est connu des autorités publiques compétentes et du personnel des prestataires de services, il est accessible et facile à utiliser. • Le système permet la soumission de comptes rendus volontaires par des individus et des organisations.

Protection des données de sécurité

SSP.SDA.03	Le niveau «Présent» signifie que:
Dans quelle mesure la législation, les politiques, les procédures et/ou les pratiques de l'État protègent-elles les données de sécurité saisies par les systèmes de comptes rendus obligatoire et volontaire de la sécurité et les sources connexes, ainsi que les informations en matière de sécurité qui en découlent?	• L'État a adopté des dispositions législatives pour protéger les données sur la sécurité, les renseignements sur la sécurité et les sources connexes. • L'État a des politiques et des procédures, y compris des accords entre les autorités de l'État, le cas échéant, pour protéger les données de sécurité, les informations sur la sécurité et les sources connexes. • Les dispositions législatives, les politiques et les procédures prévoient des exceptions pour la protection des données sur la sécurité, des renseignements sur la sécurité et des sources connexes.

Base de données ou bases de données sur la sécurité

SSP.SDA.04	Le niveau «Présent» signifie que:
Dans quelle mesure l'État a-t-il créé et tenu à jour une ou plusieurs bases de données sur la sécurité pour stocker et traiter les données pertinentes sur la sécurité, y compris les données sur les dangers et les risques pour la sécurité?	• L'État a mis en place une ou plusieurs bases de données de sécurité pour stocker et traiter les données de sécurité pertinentes, y compris les données sur les dangers et les risques pour la sécurité, qui sont proportionnées au tableau des risques de l'État. • Un mécanisme est en place pour traiter les données recueillies et tenues à jour sur les dangers et les risques pour la sécurité, y compris les données qui sont recueillies, tenues à jour et stockées dans différentes bases de données à l'échelle de l'industrie.

Identification des dangers et gestion des risques

SSP.SDA.05	Le niveau «Présent» signifie que:
Comment les données et informations contenues dans la ou les bases de données sur la sécurité sont-elles utilisées dans le cadre des processus d'identification des dangers et de gestion des risques de l'État?	• Il existe un mécanisme permettant d'utiliser les données et informations traitées, dans le cadre de l'identification des dangers et de la gestion des risques, au niveau de l'État. • Ces données et informations sont utilisées pour définir et hiérarchiser les mesures d'atténuation des risques pour la sécurité au niveau de l'État. • Un mécanisme a été mis en place pour faire en sorte que les informations servent de base à une surveillance fondée sur les risques au niveau de l'État. • Il y a un mécanisme en place pour s'assurer que l'information est reflétée dans la documentation liée au PNS. • Un mécanisme a été mis en place pour veiller à ce que les informations soient utilisées pour affiner les IPS au niveau de l'État.

Initier des actions

SSP.SDA.06	Le niveau «Présent» signifie que:
Comment l'État agit-il sur les risques de sécurité identifiés et évalue-t-il l'efficacité des mesures d'atténuation de la sécurité?	• Il existe un mécanisme qui définit quand l'État doit prendre des mesures en fonction des risques identifiés et de la nature de ces mesures. • Un mécanisme est en place pour évaluer en permanence l'efficacité des mesures d'atténuation de la sécurité prises par l'État. • Un mécanisme est en place pour évaluer l'efficacité des mesures d'atténuation, y compris l'assurance que les mesures d'atténuation n'entraînent pas de risques accrus ou n'ont pas d'incidence négative importante sur la sécurité. • Il y a un mécanisme en place pour identifier et atténuer les nouveaux risques qui peuvent être causés par des mesures d'atténuation.

- Commencez par définir quel groupe discutera des dangers/questions de sécurité identifiés.
- Utiliser une matrice de tolérance au risque.

Accès aux données et à l'information

SSP.SDA.07	Le niveau «Présent» signifie que:
Dans quelle mesure les autorités publiques participant à la mise en œuvre et à la maintenance du PNS ont-elles accès aux données et informations contenues dans la (les) base(s) de données sur la sécurité à l'appui de leurs fonctions et responsabilités?	• Il existe un mécanisme permettant d'identifier les besoins d'accès des autorités de l'État, qui participent à la mise en œuvre du PNS, aux données et informations contenues dans la ou les bases de données. • Un mécanisme a été mis en place pour faciliter l'accès des autorités publiques participant à la mise en œuvre du PNS aux données et informations contenues dans la ou les bases de données.

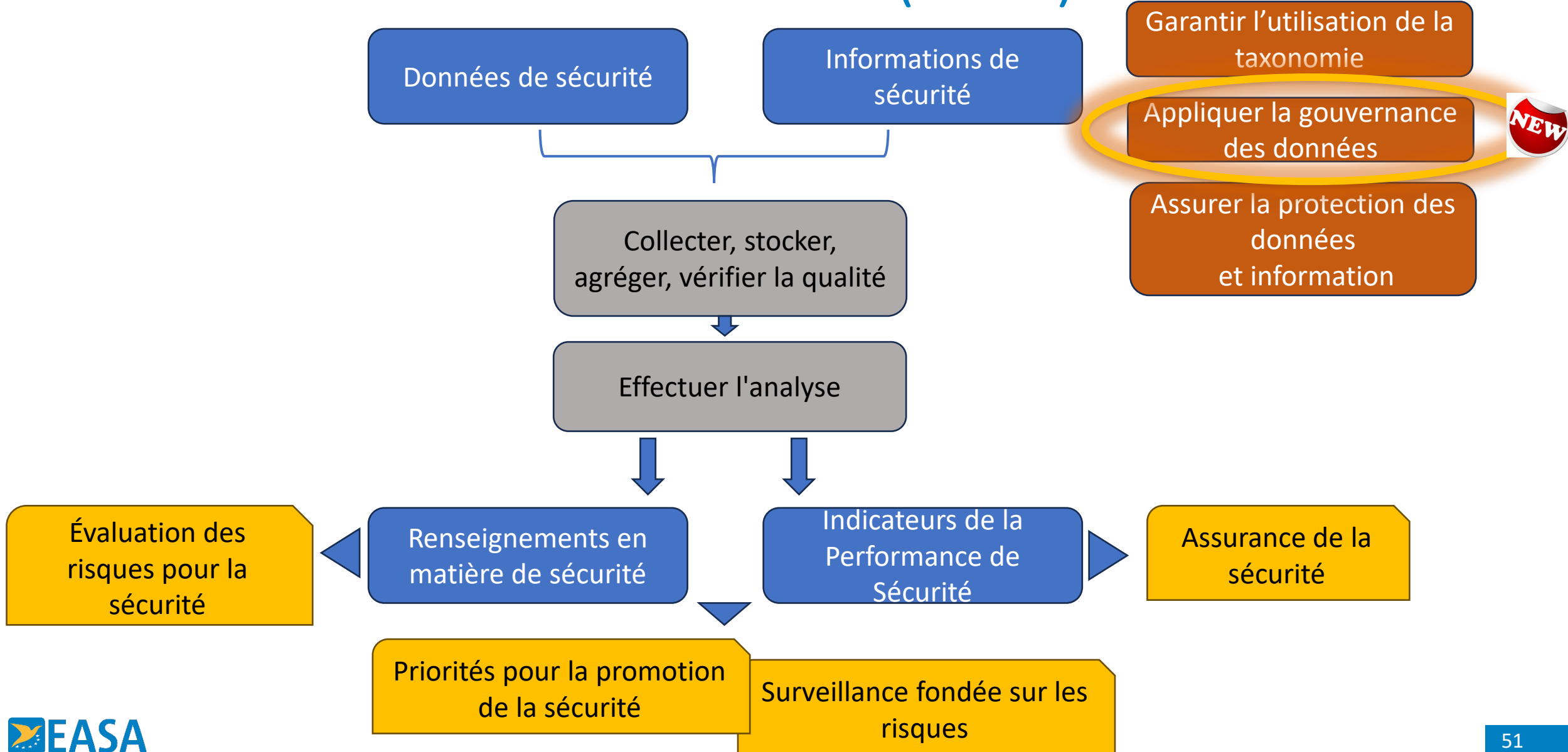
→ Le mécanisme peut être un outil informatique doté de politiques d'accès

Capacité d'analyse de la sécurité & compétences

SSP.SDA.08	Le niveau «Présent» signifie que:
Dans quelle mesure l'État a-t-il assuré la disponibilité des ressources et des compétences nécessaires pour exercer la fonction d'analyse des données de sécurité à l'appui de la gestion des risques en matière de sécurité par l'État et des activités d'assurance de la sécurité par l'État?	• Il existe un mécanisme permettant d'identifier et de définir les ressources et les compétences nécessaires pour exécuter la fonction d'analyse des données de sécurité à l'appui de la gestion des risques en matière de sécurité par l'État et des activités d'assurance de la sécurité par l'État. • Un mécanisme a été mis en place pour s'assurer que le personnel responsable de la collecte, du stockage, du traitement et de l'analyse des données possède les compétences nécessaires pour s'acquitter de ses fonctions. • Un mécanisme est en place pour veiller à ce que les différentes ressources (c'est-à-dire les outils informatiques) soient mises à la disposition du personnel concerné qui est responsable de la collecte, du stockage, du traitement et de l'analyse des données de sécurité.

- Recommandation d'inclure le personnel impliqué dans l'analyse de la sécurité dans l'analyse globale des besoins en formation pour le PNS/SGS;
- Quels outils informatiques sont envisagés pour effectuer l'analyse des données de sécurité?

Système de collecte et de traitement des données de Sécurité (SDCPS)



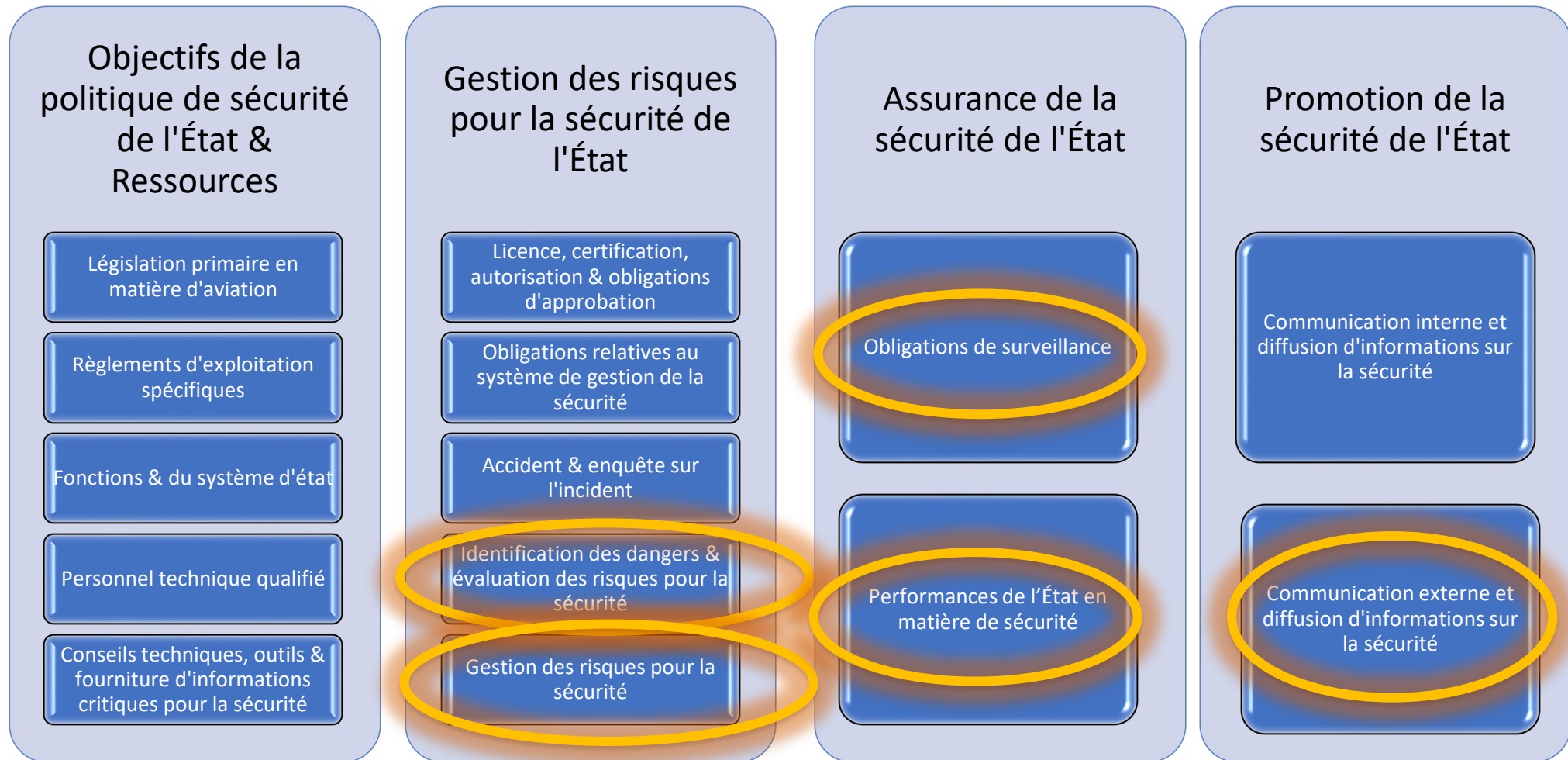
Utilisation de l'intelligence sur la sécurité pour répondre aux questions suivantes:

- Quels sont les risques les plus critiques pour la sécurité dans l'ensemble du système aéronautique de l'Etat?
- Les règlements actuels tiennent-ils suffisamment compte du/des risques?
- Où l'État doit-il agir en priorité?
- Quels risques/problèmes de sécurité sont à traiter par les prestataires de services?

Objectif de l'analyse des données de sécurité

- Comprendre le risque, identifier les facteurs de causalité et leur fréquence
- Analyser les précurseurs d'accidents, identifier de manière proactive et hiérarchiser les questions de sécurité
- Suivi de l'efficacité des mesures d'atténuation des risques
- Mise en œuvre d'une surveillance fondée sur les risques et les performances
- Surveillance des performances en matière de sécurité
- Maintenir une sensibilisation aux risques pour la sécurité dans le système aéronautique
- Soutenir la définition des mesures d'atténuation des risques
- Soutenir la mise en place et le maintien de la cartographie des risques de l'État

PNS : Où les données de sécurité sont-elles le plus nécessaires?



La plupart des accidents ont des « précurseurs »

Les facteurs étaient visibles lors d'incidents ou d'accidents antérieurs

Est-il possible de prévoir les accidents à partir d'incidents?

L'iceberg...

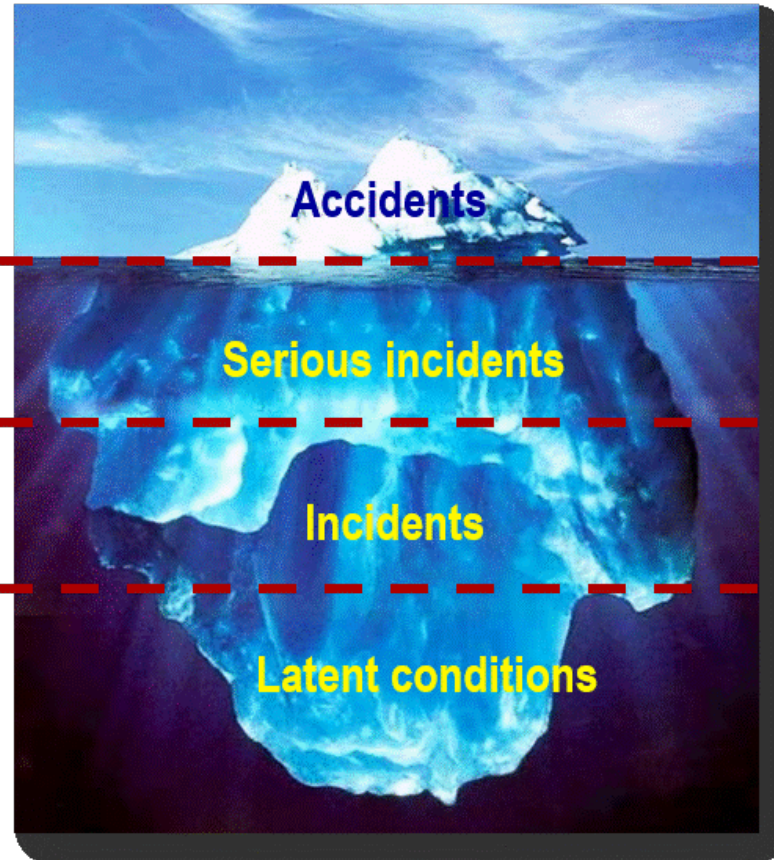
Number of occurrences

1 – 5

30 – 100

100 – 1000

1000 – 4000



Accidents

Serious incidents

Incidents

Latent conditions

réactif

proactif

précurseurs d'accidents

Exemple

Défaillance du radioaltimètre pendant l'approche de Schiphol

Reconstruction animée

Lecture radio-altimètre négative

Activation du mode auto-manette « retard flare »



B737-800 Amsterdam, 25 février 2009, 9 Décès (source:
Rapport d'accident du Bureau néerlandais de la sécurité)

B737-800 Amsterdam, 25 février 2009, 9 décès

[...] deux incidents ont fait l'objet de discussions au sein du comité d'examen de la sécurité de Boeing en 2004, au cours desquels le mode «retard d'auto-manette» a été activé à 2100 pieds et 1200 pieds respectivement, à la suite de lectures négatives du système de radio-altimètre.

Cela montre également que Boeing était conscient de la possibilité de l'apparition des conséquences spécifiques qui se sont produites dans ce cas particulier.

Suite à l'analyse statistique et à l'exécution des essais sur simulateur de vol, Boeing a conclu qu'il ne s'agissait pas d'un problème de sécurité, car, entre autres, les pilotes ont reçu des avertissements et des notifications adéquats pour leur permettre d'intervenir à temps, afin de rétablir la situation et d'atterrir en toute sécurité.

B737-800 Amsterdam, 25 février 2009, 9 décès

Les problèmes avec les systèmes de radioaltimètre dans la flotte de Boeing 737-800 avaient affecté plusieurs compagnies aériennes, y compris Turkish Airlines, pendant de nombreuses années et étaient connus de Boeing et de la FAA.

Plusieurs compagnies aériennes, dont Turkish Airlines, considéraient les problèmes liés aux systèmes de radioaltimètres comme un problème technique plutôt que comme un danger pour la sécurité des vols. Par conséquent, les pilotes n'ont pas été informés de ce problème.

Malgré le fait que Boeing et la FAA savaient depuis de nombreuses années que le système de radioaltimètre causait de nombreux problèmes et affectait le fonctionnement d'autres systèmes, cette situation n'a pas été désignée comme un risque pour la sécurité.

L'analyse des données de sécurité peut contribuer à la prévention des accidents

Uniquement
si :

l'analyse est basée sur les bonnes données

l'analyse est correctement menée

les résultats de l'analyse parviennent aux bonnes organisations/personnes

la criticalité de ces résultats est 'prise au sérieux' par les décideurs

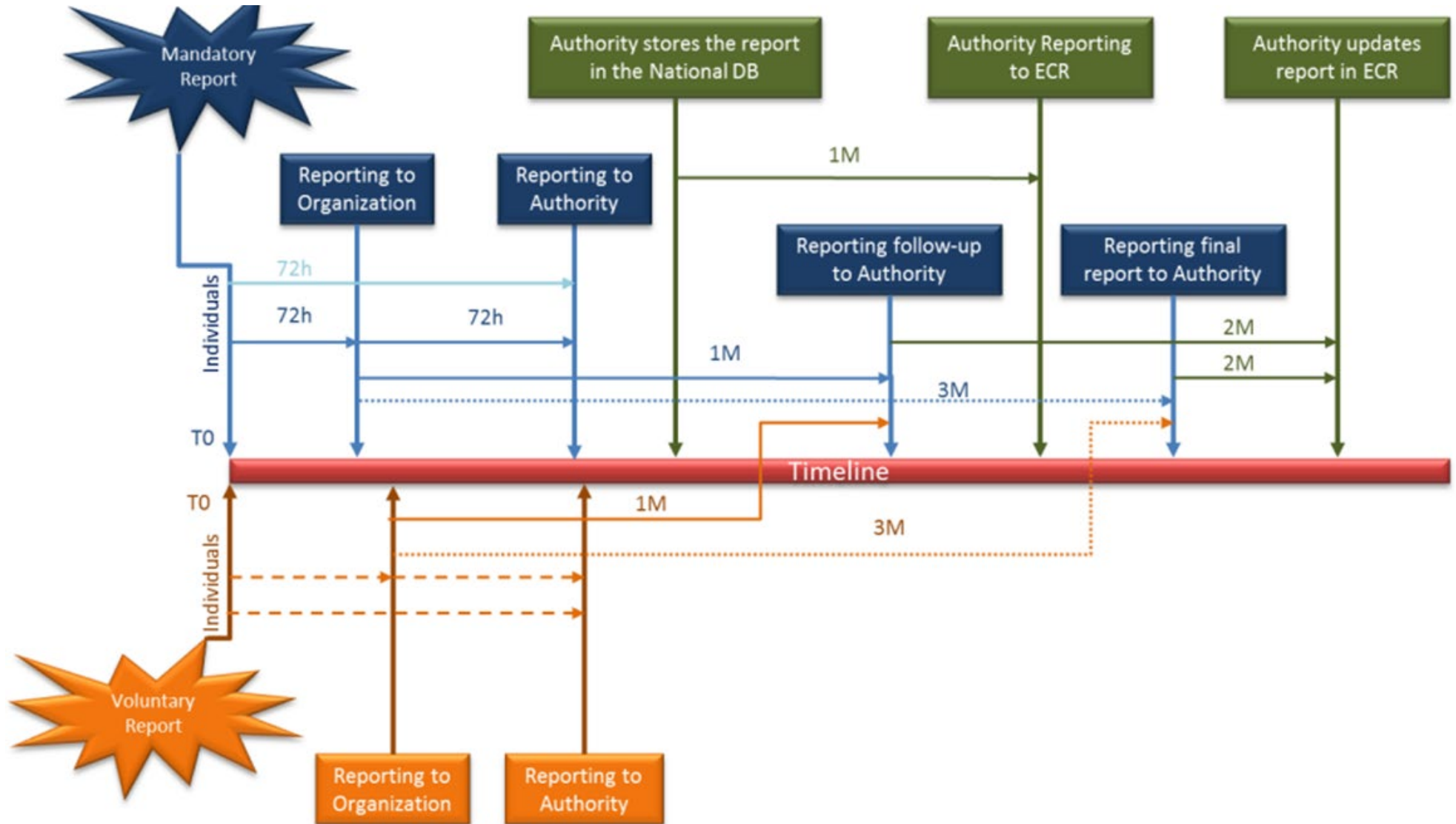
les mesures de sécurité appropriées sont prises.

Systèmes de comptes rendus d'événements

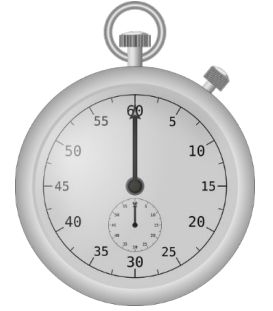
- Systèmes de comptes rendus obligatoires
 - Systèmes de comptes rendus volontaires
 - Systèmes de comptes rendus confidentiels
 - Systèmes automatiques de collecte de données (FDM)
-
- Comptes rendus interne au sein d'une organisation (SGS)
 - Comptes rendus entre organisations et autorités (PNS)
 - Comptes rendus des particuliers vers l'autorités (PNS)
 - Comptes rendus entre les organisations (SGS)
 - Etc...

Cheminement des comptes rendus et delais

Example: Europe



Union Européenne – la règle des 72 heures



- ✓ La «règle des 72 heures» est parfois source de confusion: quand le temps commence-t-il à être décompté?
 - ✓ En principe, chaque déclarant dispose de 72 heures pour se présenter à l'organisation suivante de la chaîne une fois qu'il s'est rendu compte qu'il y a eu un événement.
 - ✓ Pas la même chose que 72 heures à partir du moment où l'événement s'est produit.
 - ✓ L'organisation doit mettre en place un examen périodique (quotidien... hebdomadaire...) des rapports de sécurité pour identifier les événements à signaler à l'Autorité
 - ✓ Dans certains cas, une enquête plus approfondie pourrait être nécessaire avant de décider si un compte rendu obligatoire est nécessaire
- ✓ Il est important de mettre en place un processus régulier d'identification des événements qui doivent faire l'objet d'un rapport obligatoire d'occurrence

Qu'est-ce qu'une taxonomie?

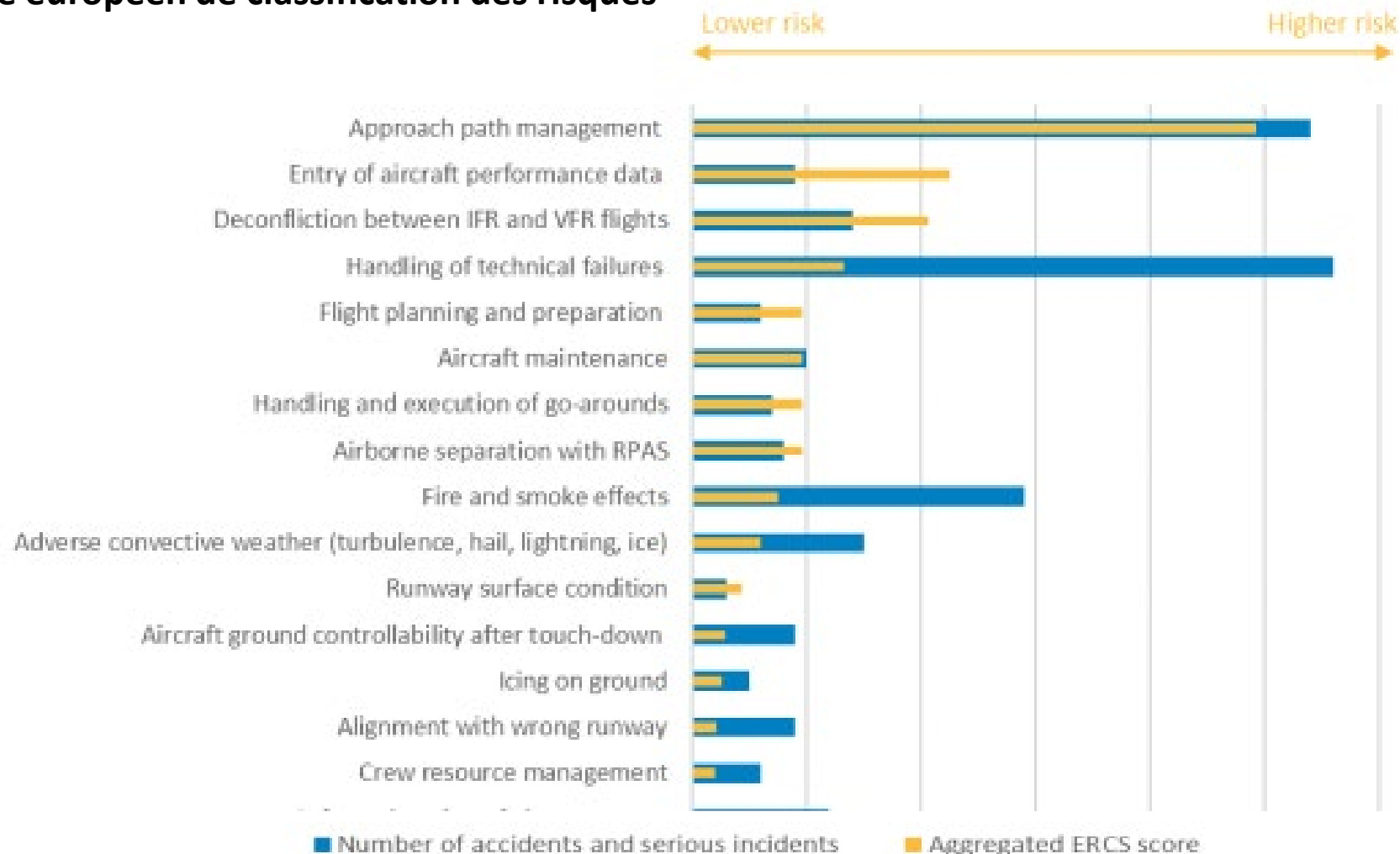
- Une taxonomie est simplement une version réduite d'un langage, utilisée pour créer des données catégoriques à partir d'informations.
- Exemples dans le domaine de l'aviation:
 - Catégories d'événements de l'Équipe de sécurité de l'aviation commerciale/Équipe commune de taxonomie de l'OACI (CICTT)
 - Déclaration des données sur les accidents/incidents (ADREP)
 - Système d'analyse et de classification des facteurs humains (HFACS)
- Il n'existe pas de taxonomie parfaite

Pourquoi coder les données d'occurrence?

- Pour aider à répondre à des questions comme
 - À quelle fréquence un certain phénomène se retrouve-t-il dans les données?
 - Un certain phénomène se retrouve-t-il dans les données?
 - Quels phénomènes se retrouvent dans les données?
- Les données codées sont déjà des informations
- Peut être indépendant de la langue utilisée
- Permet l'analyse statistique de grandes quantités de données textuelles

Données d'événement codées – exemple ASR 2023 de l'AESA

ERCS = Système européen de classification des risques



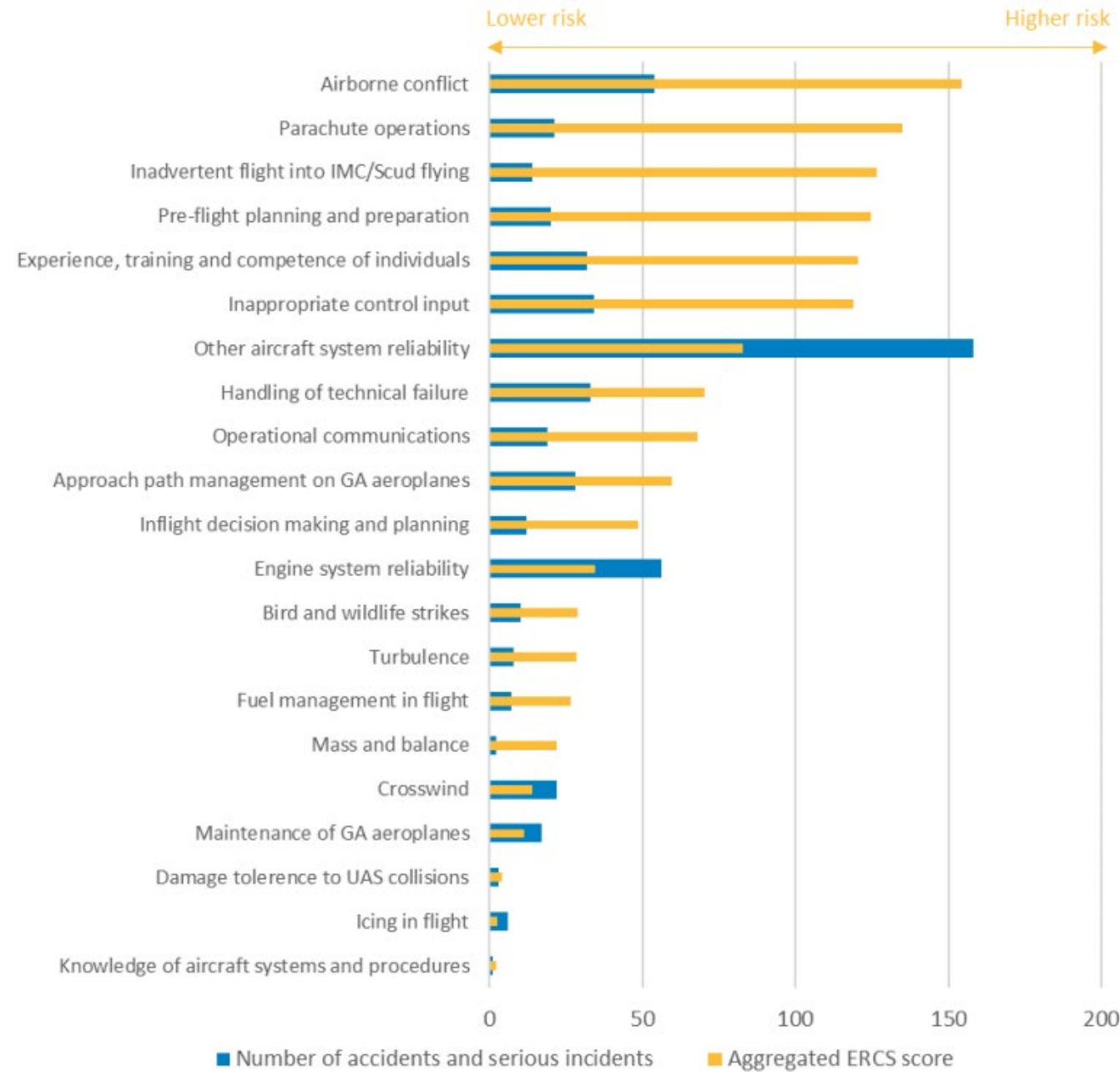
Appendix 2 Figure 1 Safety issues by aggregated ERCS score and numbers of accidents and serious incidents involving CAT complex aeroplanes and NCC aeroplanes

Données d'événement codées

exemple ASR 2023 de l'AESA

Safety Issues by aggregated ERCS score and numbers of accidents
and serious incidents involving NCO aeroplanes

NCO = Non-Commercial other than complex motor-powered aircraft



Problématiques de sécurité ('*Safety Issues*')

- Les problèmes de sécurité sont des manquements à la sécurité liés à un ou plusieurs dangers. Ils sont la manifestation réelle d'un danger ou d'une combinaison de plusieurs dangers dans un contexte spécifique (méthodologie ARMS). La problématique de sécurité a été identifiée par le processus systématique d'identification des dangers de l'organisation.
- Une problématique de sécurité pourrait être
 - une implication locale d'un danger
 - par exemple, problèmes de dégivrage dans un type particulier d'aéronef ou
 - une combinaison de dangers dans une partie de l'opération
 - par exemple, l'exploitation d'un aéroport exigeant.
- Les problèmes de sécurité peuvent faire l'objet d'une évaluation des risques et d'une gestion pratique (atténuation).

Identification des problèmes de sécurité

- Afin d'identifier les problèmes de sécurité, l'analyse peut être effectuée à différents niveaux d'agrégation, par exemple:
 - Au niveau d'un secteur de l'aviation
 - exemples:
 - Exploitation d'hélicoptères en mer (offshore helicopter operations)
 - Avions de Transport Commercial
 - Aviation Générale
 - Au niveau d'une catégorie d'accident (ICAO GASP: Catégorie d'occurrence à risque élevé / HRC)
 - exemple:
 - Perte de contrôle en vol (LOC-I)
 - Incursion sur piste (RI)

Analyse au niveau d'une catégorie d'accident

- *À quelles questions voulons-nous répondre?*
 - Quels sont les événements pertinents?
 - Quels sont les principaux scénarios d'accidents?
 - Quels sont les principaux facteurs contributifs?
 - Quels sont les principaux problèmes de sécurité sous-jacents?

Quelles sont les principales catégories d'accidents?

→ L'édition 2023-2025 du GASP définit les catégories d'événements à risque élevé dans le monde (G-HRC) comme suit :

Perte de contrôle en vol

- LOC-I

Collision en vol

- MAC

Sortie de piste

- RE

Incursion sur piste

- RI

Impact sans perte de contrôle

- CFIT

European Key Risk Areas (KRAs)

1. [Airborne collision](#): a collision between aircraft while both aircraft are airborne; or between aircraft and other airborne objects (excluding birds and wildlife).
2. [Aircraft upset](#): an undesired aircraft state characterised by unintentional divergences from parameters normally experienced during operations, which might ultimately lead to an uncontrolled impact with terrain.
3. [Collision on runway](#): a collision between an aircraft and another object (other aircraft, vehicles, etc.) or person that occurs on a runway of an aerodrome or other predesignated landing area. This does not include collisions with birds or wildlife.
4. [Excursion](#): an occurrence when an aircraft leaves the runway or movement area of an aerodrome or landing surface of any other predesignated landing area, without getting airborne. This includes high-impact vertical landings for rotorcraft/VTOL and balloons/airships.
5. [Fire, smoke and pressurisation](#): an occurrence involving cases of fire, smoke, fumes or pressurisation situations that may become incompatible with human life. This includes occurrences involving fire, smoke or fumes affecting any part of an aircraft, in flight or on the ground, which is not the result of impact or malicious acts.
6. [Ground damage](#): damage to aircraft induced by operation of aircraft on ground on any other ground area than a runway or predesignated landing area, as well as damage during maintenance.
7. [Obstacle collision in flight](#): collision between an airborne aircraft and obstacles raising from the surface of the earth. Obstacles include such things as tall buildings, trees, power cables, telegraph wires and antennae as well as tethered objects.
8. [Terrain collision](#): an occurrence where an airborne aircraft collides with terrain, without indication that the flight crew was unable to control the aircraft. This includes instances when the flight crew is affected by visual illusions or degraded visual environment.
9. [Other injuries](#): an occurrence where fatal or non-fatal injuries have been inflicted, which cannot be attributed to any other key risk area.
10. [Security](#): an act of unlawful interference against civil aviation. This includes all incidents and breaches related to surveillance and protection, access control, screening, implementation of security controls and any other acts intended to cause malicious or wanton destruction of aircraft and property, endangering or resulting in unlawful interference with civil aviation and its facilities. It includes both physical and cybersecurity events

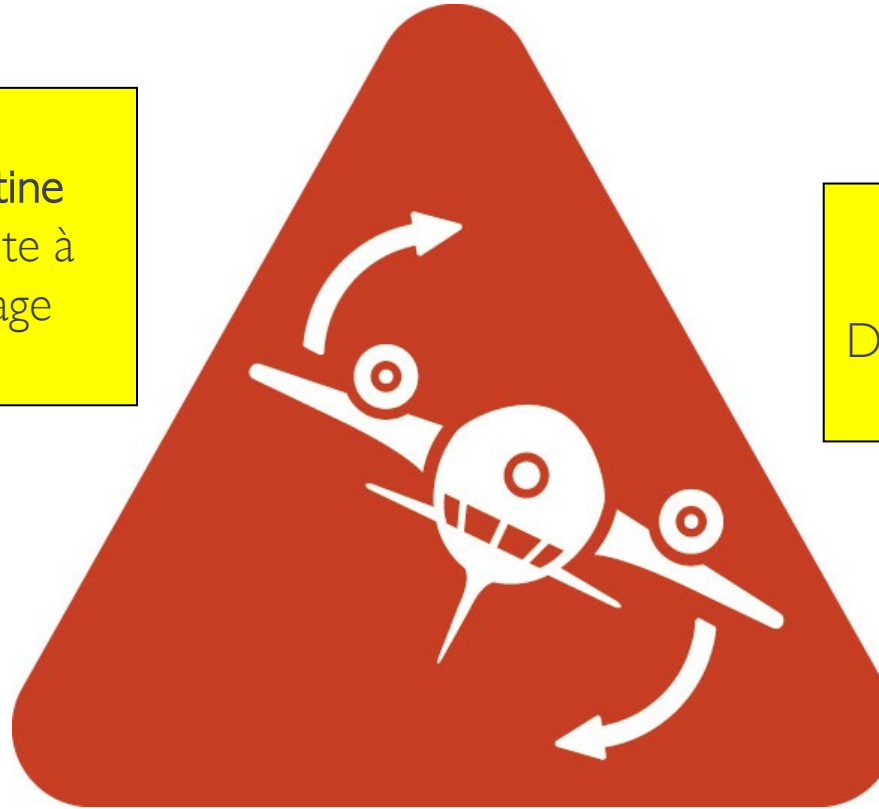
Exemple d'accidents: Perte de contrôle en vol

18 mai 2011
Saab 340 en Argentine
Perte de contrôle suite à
Conditions de givrage
22 Décès

27 janvier 2001
[Shorts 360 pour Forth Estuary](#)
LOC & amerrissage forcé
2 Décès

1er juin 2009
A330 Océan Atlantique Sud
Décrochage et LOC en croisière
228 décès

28 décembre 2014
A320 en Indonésie
L'avion a perdu de la hauteur, a
décroché
162 décès

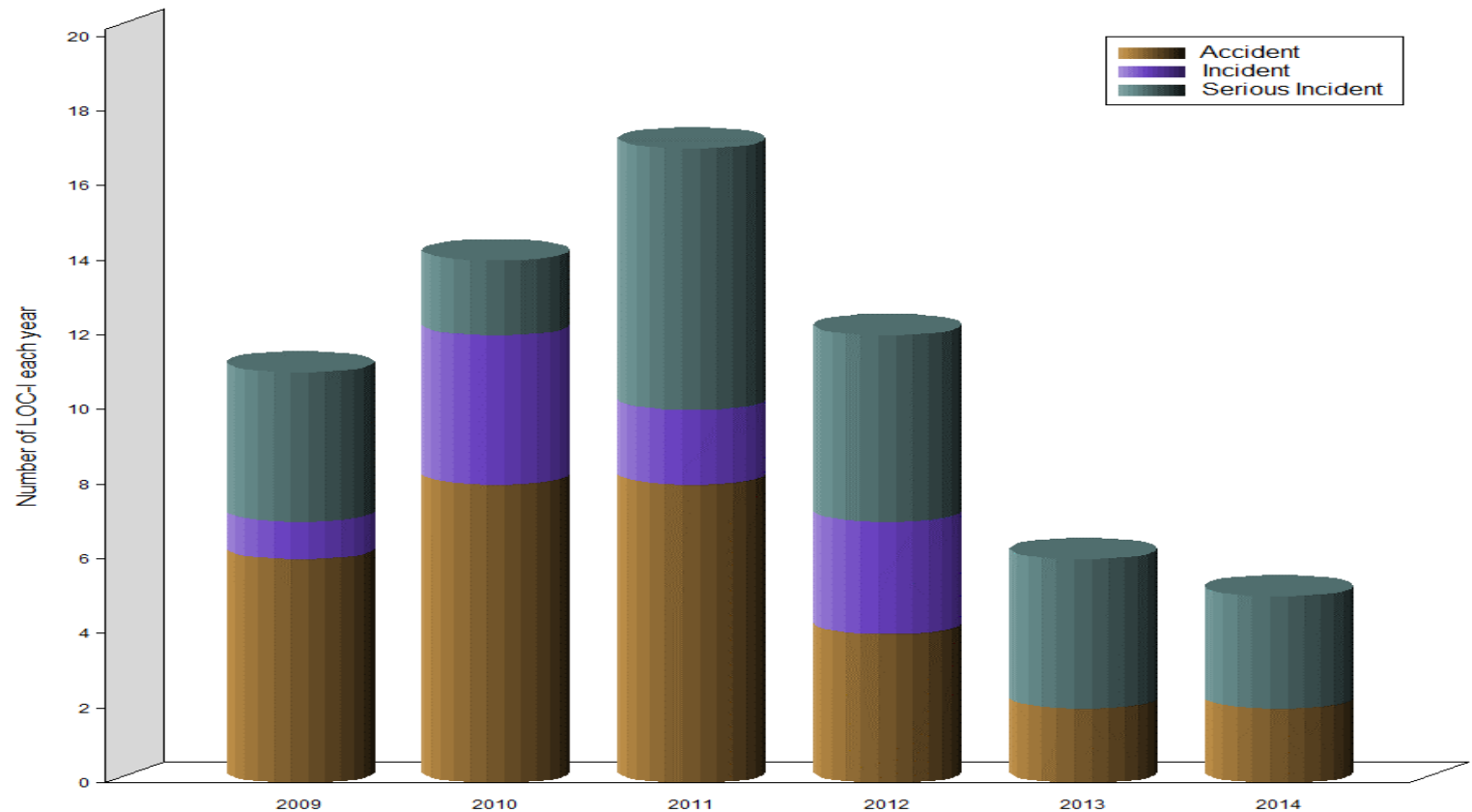


29 avril 2013
B747 en Afghanistan
Perte de maîtrise au décollage
En raison du changement du centre
de gravité
7 Décès



Étude LOC-I EASA -> *Quels sont les événements pertinents?*

- Événements de la LOC-I entre 2009 et 2014
- Avions à voilure fixe
- MTOW supérieur à 5,700 kg; Transport aérien commercial
- 65 événements

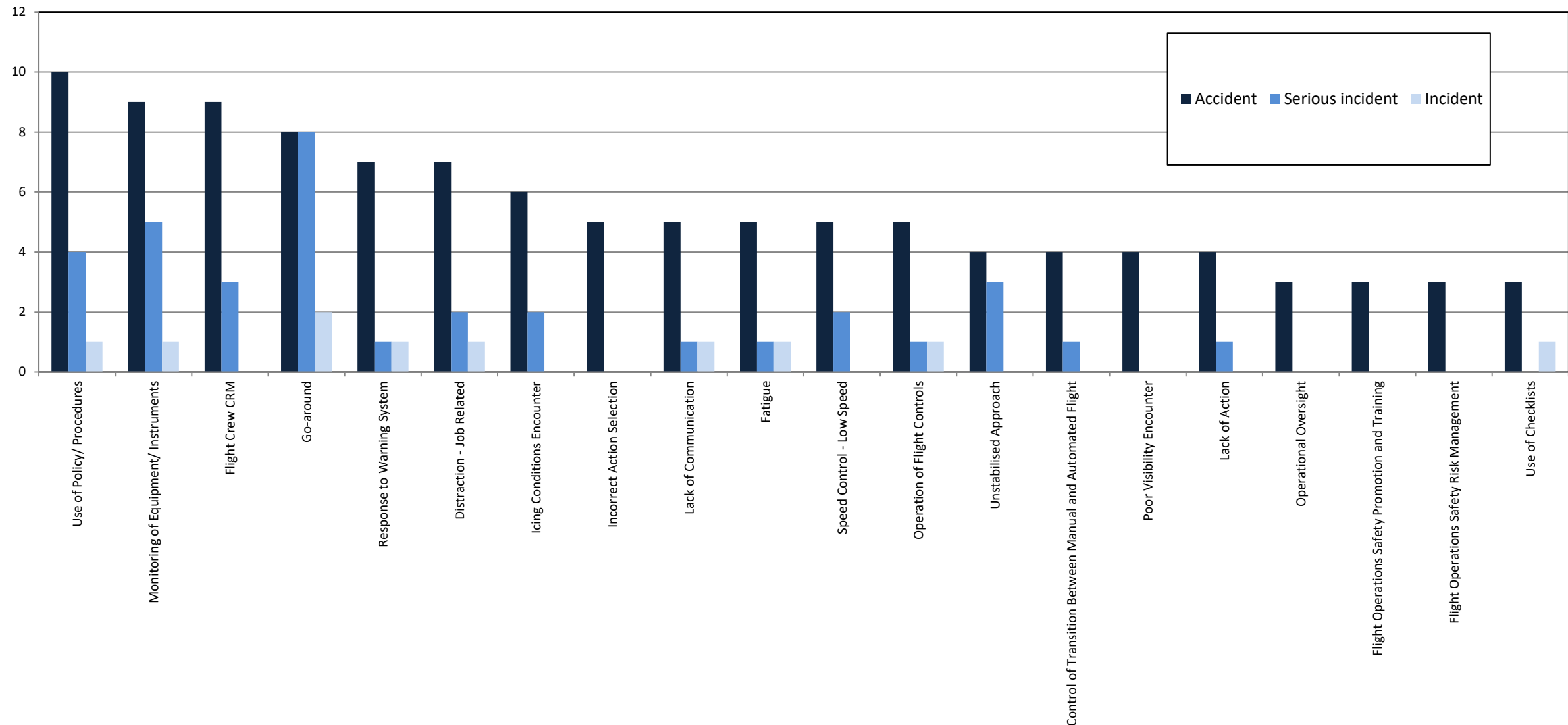


LOC-I- Quels sont les principaux scénarios?

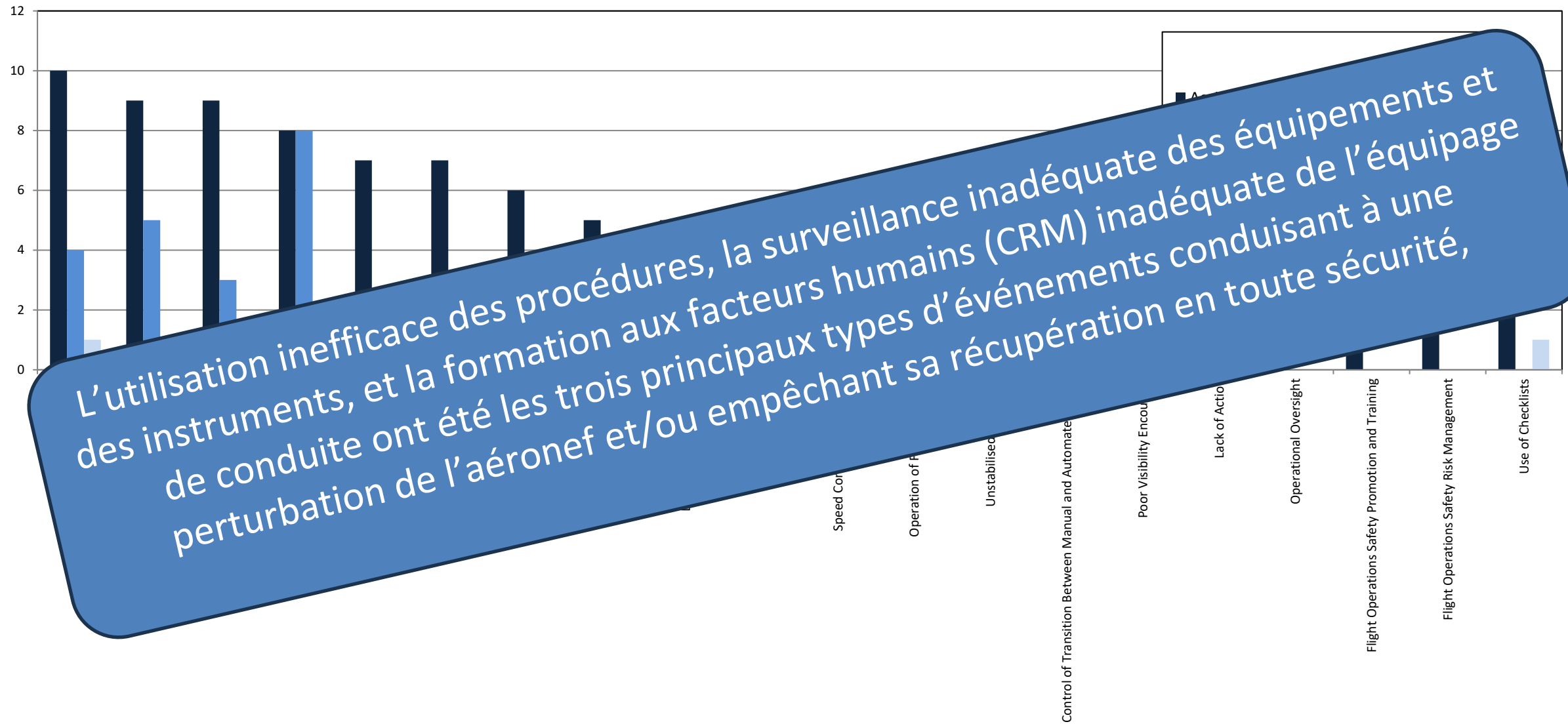
- Environnement
 - givrage
 - cisaillement du vent
 - turbulence
- Techniques
 - défaillances de système
- Autres
 - chargement
 - action de l'équipage
 - Etc.

Identifiés à partir des rapports d'événements
La qualité des rapports est essentielle

Facteurs les plus récurrents dans les accidents LOC-I:



Facteurs les plus récurrents dans les accidents LOC-I:



Définition Culture de sécurité (il existe de nombreuses définitions différentes)

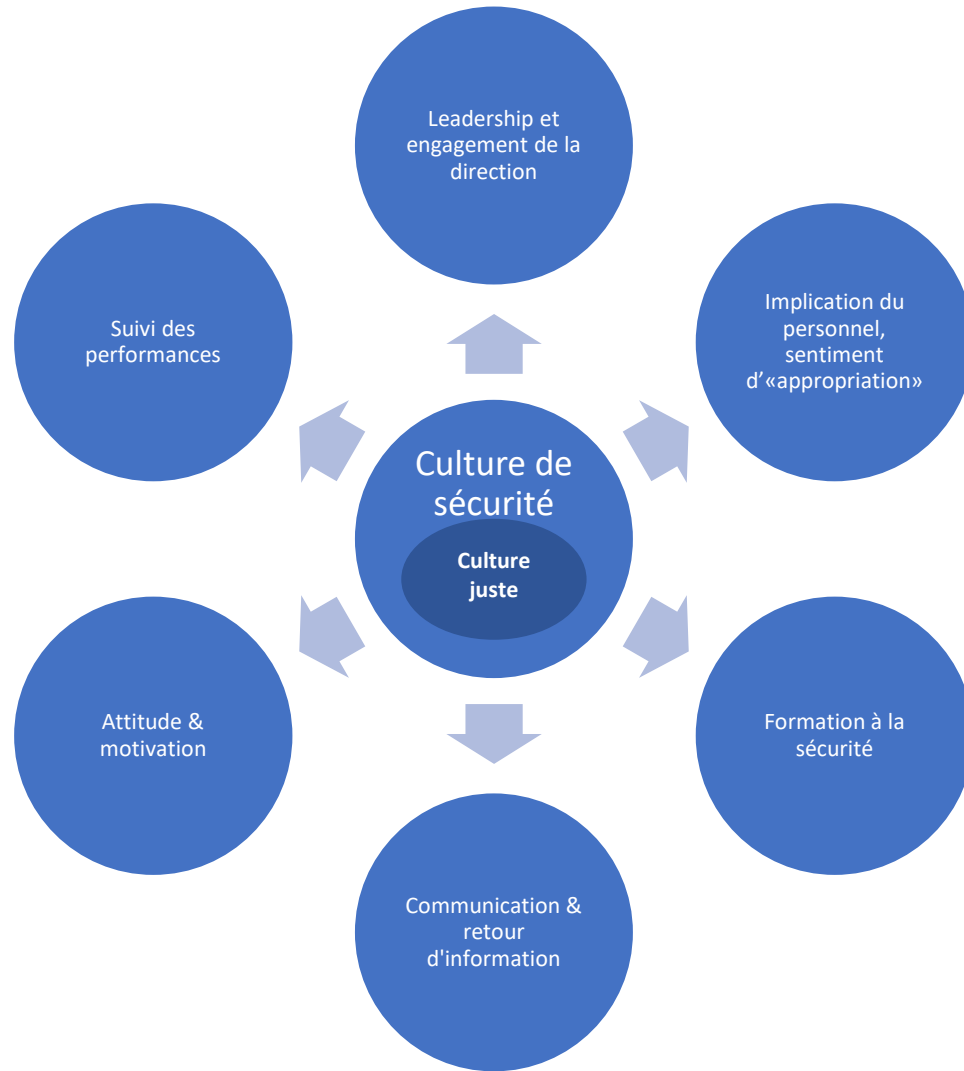
L'Annexe 19 ne fournit aucune

***Culture de sécurité:** Ensemble durable de valeurs, de normes, d'attitudes et de pratiques au sein d'une organisation soucieuse de minimiser l'exposition de la main-d'œuvre et du grand public à des conditions dangereuses. Dans une culture de sécurité positive, une préoccupation, un engagement et une responsabilisation communs en matière de sécurité sont encouragés.*

Source : CASA (Australie)

La culture de la sécurité ne peut pas être imposée par la loi. L'Annexe 19 exige que les États et les prestataires de services promeuvent une culture positive de la sécurité pour soutenir une mise en œuvre efficace des PNS/SGS.

La culture de la sécurité est le «catalyseur» des SGS



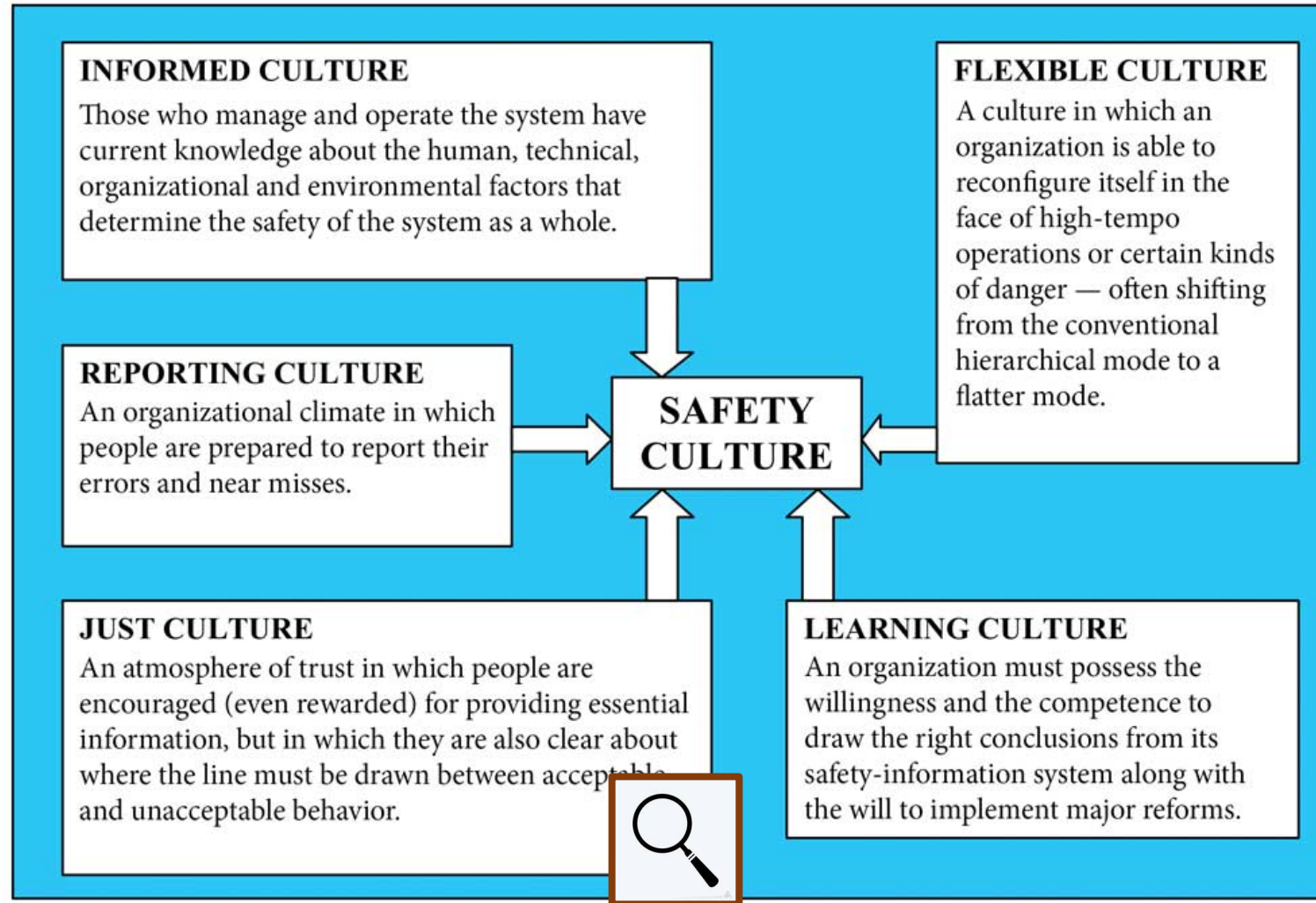
La culture de sécurité est la façon dont la sécurité est perçue, valorisée et priorisée dans une organisation.

Il reflète l'engagement réel en faveur de la sécurité à tous les niveaux de l'organisation. Plus la culture de la sécurité sera bonne, plus l'organisation sera en mesure de «tirer dans des poches d'informations de sécurité».

Elle est souvent influencée par les attitudes & des supérieurs hiérarchiques à l'égard de la sécurité.

La culture juste est un sous-ensemble de la culture de la sécurité.

Les modèles de culture de sécurité décomposent cela en différentes «dimensions» (caractéristiques)



Modèle de culture de sécurité selon le professeur James Reason

Définitions

Culture juste: Une culture dans laquelle les opérateurs de première ligne ou d'autres personnes ne sont pas punis pour des actions, des omissions ou des décisions prises par eux qui sont à la mesure de leur expérience et de leur formation, mais dans laquelle la négligence grave, les violations délibérées et les actes destructeurs ne sont pas tolérés.

Source : Règlement (UE) no 376/2014 «Rapports d'événements»

Il s'agit d'équilibrer la
sécurité et la responsabilité



JUST CULTURE – Équilibrer la sécurité et la responsabilité – Sidney Dekker, 2007

Culture juste et équitable

- Protection des personnes qui signalent et des personnes mentionnées dans le rapport
- Règles relatives à la confidentialité de l'identité
- S'abstenir d'intenter une action et limiter les informations utilisées dans le cadre d'une procédure
- Protection contre les préjudices de la part de l'employeur
- En Europe, les organisations doivent adopter une politique interne de culture juste
 - possibilité pour les employés de faire appel

Just Culture in an Organization



Just Culture - Because We Are All Humans

Ana Maria Stoica



<https://skybrary.aero/video/just-culture-organization>

Comment mettre en œuvre les principes de la culture juste?

- Au niveau des prestataires de services
 - Définir les responsabilités et une procédure pour déterminer ce qui est acceptable et ce qui ne l'est pas.
 - Ce type de décision doit se faire avec la participation des représentants/syndicats du personnel.
- Exemple d'aide à la décision:
 - *Modèle Baines Simmons FAIR*

Téléchargement gratuit



Marqueurs d'une culture de sécurité positive

un engagement visible de la direction - la direction motive activement son personnel à prendre soin de la sécurité et crée des conditions de travail favorables à la sécurité

la contribution du personnel est activement encouragée – la direction reste ouverte aux mauvaises nouvelles

le personnel et la direction restent conscients des risques, même lorsque les performances sont élevées

le personnel reçoit des informations pertinentes en matière de sécurité et un retour d'information est demandé

il existe un moyen convenu de faire la distinction entre un comportement acceptable et un comportement inacceptable

Culture de sécurité - sources d'information (en Anglais)

SMICG

- Outil et ligne directrice d'évaluation de la culture de sécurité de l'industrie
- Outil d'auto-évaluation de la culture organisationnelle pour les organismes de réglementation

EUROCONTROL

- Boîte à outils d'amélioration de la culture de sécurité pour l'ATM
- Boîte à outils: Penser les systèmes pour la sécurité: Dix principes



Points Clés concernant la culture de la sécurité:

→ Culture de sécurité

- constitue le catalyseur de la gestion de la sécurité
- ne peut pas être directement réglementée
- peut être influencée et parfois endommagée par le régulateur
- n'est pas facile à mesurer, mais peut être évaluée

→ Les autorités aéronautiques peuvent envisager d'évaluer

- La culture de la sécurité au niveau de l'industrie
- leur propre culture de sécurité



safety.management@easa.europa.eu

easa.europa.eu/connect



Your safety is our mission.

An agency of the European Union 