



JOUR 2

## Certified ISO/IEC 42001 Lead Implementer

PECB

© Professional Evaluation and Certification Board, 2024. Tous droits réservés.

Version1.0

Numéro de document: AIMSLID2V1.0

Les documents fournis aux participants sont strictement réservés à des fins de formation. Aucune partie de ces documents ne peut être publiée, distribuée, affichée sur Internet ou sur un intranet, extraite ou reproduite sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris par photocopie, sans l'autorisation écrite préalable de PEBC.

# Programme de la formation

## Section 8

L'organisme et son contexte

## Section 11

Politique d'IA

## Section 9

Périmètre du SMIA

## Section 12

Management du risque lié à l'IA

## Section 10

Analyse du système existant

## Section 13

Déclaration d'applicabilité

PECB

2

À l'issue de cette journée, les participants seront capables:

- D'identifier les facteurs internes et externes, les processus clés et les parties intéressées impliquées dans la mise en œuvre d'un SMIA
- De déterminer les éléments clés du périmètre du SMIA, couvrant les limites organisationnelles, du système d'information, et physiques
- D'élaborer la politique d'IA et des politiques spécifiques en matière d'IA
- D'établir un processus de management des risques et d'effectuer des appréciations du risque
- De passer en revue et de sélectionner les mesures d'IA applicables et d'élaborer une Déclaration d'applicabilité (DdA)

# Section 8

## L'organisme et son contexte

- Mission, objectifs, valeurs et stratégies de l'organisme
- Objectifs du SMIA
- Définition préliminaire du périmètre
- Environnement interne et externe
- Principaux processus et activités
- Parties intéressées
- Exigences métier

PECB

3

La présente section fournira des informations qui aideront le participant à comprendre l'importance de l'identification des facteurs internes et externes qui peuvent influer sur la mise en œuvre d'un SMIA, les processus clés et les parties intéressées impliquées dans la mise en œuvre d'un SMIA, ainsi que les informations requises pour planifier la mise en œuvre du SMIA.

# L'organisme et son contexte

1. Définir et établir		2. Mettre en œuvre et opérer		3. Surveiller et revoir		4. Maintenir et améliorer	
1.1	Leadership et approbation du projet	2.1	Sélection et conception des mesures	3.1	Surveillance, mesurage, analyse et évaluation	4.1	Traitement des non-conformités
1.2	Rôles et responsabilités	2.2	Mise en œuvre des mesures	3.2	Audit interne	4.2	Amélioration continue
1.3	<b>L'organisme et son contexte</b>	2.3	Gestion des informations documentées	3.3	Revue de direction		
1.4	Périmètre du SMIA	2.4	Communication				
1.5	Analyse du système existant	2.5	Compétence et sensibilisation				
1.6	Politique d'IA	2.6	Gestion des opérations d'IA				
1.7	Management du risque lié à l'IA						
1.8	Déclaration d'applicabilité						

PECB

4

# Les exigences d'ISO/IEC 42001 en termes de contexte de l'organisme

ISO/IEC 42001, articles 4.1, 4.3 et 4.4

*L'organisme doit déterminer les enjeux externes et internes pertinents compte tenu de sa mission et qui ont une incidence sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son système de management de l'IA.*

*Pour établir le périmètre du système de management de l'IA, l'organisme doit en déterminer ses limites et son applicabilité.*

*L'organisme doit établir, mettre en œuvre, maintenir et améliorer et documenter en continu un système de management de l'IA, y compris les processus nécessaires et leurs interactions, en accord avec les exigences du présent document.*

PECB

5

# 1.3 L'organisme et son contexte

## Liste des activités

1.3.1

Comprendre la mission, les objectifs, les valeurs et les stratégies

1.3.5

Identifier les principaux processus et activités

1.3.2

Déterminer les objectifs du SMIA

1.3.6

Identifier et analyser les parties intéressées

1.3.3

Déterminer le périmètre préliminaire

1.3.7

Identifier et analyser les exigences métier

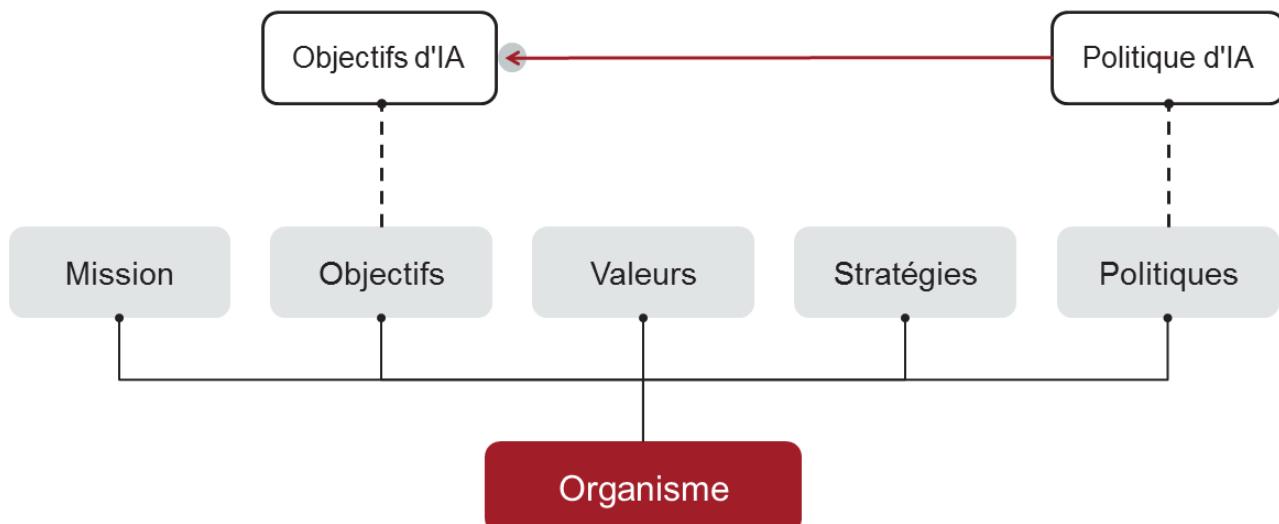
1.3.4

Analyser l'environnement interne et externe

PECB

6

### 1.3.1 Comprendre la mission, les objectifs, les valeurs et les stratégies



PECB

7

Il est nécessaire d'obtenir une vue d'ensemble de l'organisme afin de comprendre les défis en matière de management de l'IA auxquels il est confronté et le risque inhérent à ce segment de marché. Des informations générales sur l'organisme devraient être recueillies afin de mieux comprendre sa mission, ses stratégies, ses principaux objectifs, ses valeurs, etc. La cohérence et l'alignement entre les objectifs stratégiques établis pour l'IA et la mission de l'organisme en sont ainsi facilités.

**Mission:** La mission est ce qui justifie et définit l'existence de l'organisme. Elle sert de point de référence pour que tout le monde sache où va l'organisme.

**Implications pour le management de l'IA:** Le management de l'IA vise à aider l'organisme à remplir sa mission, qui comprend l'utilisation, la conception, le développement et la fourniture responsables de systèmes d'IA dignes de confiance. Le SMIA doit donc être aligné sur la mission de l'organisme.

**Valeurs:** Les valeurs sont les convictions fondamentales et durables qui sont partagées par les membres de l'organisme et qui influencent le comportement des individus.

**Implications pour le management de l'IA:** Les valeurs de l'organisme influencent les choix faits par les professionnels du management de l'IA. À titre d'exemple, les valeurs peuvent influencer les priorités et les politiques en termes d'évaluation du risque de l'IA et de problématiques d'éthique.

**Objectifs:** Les objectifs sont le résultat que l'organisme veut atteindre. Les objectifs sont généralement prédéterminés, quantifiés et limités dans le temps (par exemple, améliorer de 10% la fiabilité du système d'IA au cours des 12 prochains mois).

**Implications pour le management de l'IA:** Concernant la stratégie, le SMIA doit être aligné sur les objectifs de l'organisme afin d'atteindre l'objectif final et d'assurer une utilisation, une conception, un développement et une fourniture responsables de systèmes d'IA dignes de confiance.

**Stratégies:** La stratégie consiste en une séquence définie d'actions visant à atteindre un ou plusieurs objectifs.

**Implications pour le management de l'intelligence artificielle:** Le choix et les résultats des actions dépendront également de la stratégie de management de l'IA définie par l'organisme.

## 1.3.2 Déterminer les objectifs du SMIA

1

### Management du risque amélioré

La mise en œuvre du SMIA peut-elle améliorer le management du risque ?

2

### Management efficace de l'IA

La mise en œuvre du SMIA peut-elle améliorer le développement et le management des systèmes d'IA ?

3

### Avantage concurrentiel

La mise en œuvre d'un SMIA peut-elle procurer un avantage concurrentiel ?

PECB

8

### **ISO/IEC 42001 article 4.1 Compréhension de l'organisme et de son contexte**

*L'organisme doit tenir compte de la finalité visée par les systèmes d'IA qu'il développe, fournit ou utilise.*

Les objectifs d'un SMIA sont l'expression de l'intention de l'organisme de traiter les risques identifiés et de se conformer aux exigences fixées. Néanmoins, il est nécessaire d'établir d'abord les objectifs du SMIA avec les parties intéressées.

Ces objectifs du SMIA sont nécessaires à la détermination du périmètre et devront être validés au plus haut niveau de l'organisme. Les objectifs peuvent être affinés en cours de projet, particulièrement après la réalisation de l'analyse du risque. Les objectifs doivent être correctement documentés.

# Planification des objectifs d'IA :

## ISO/IEC 42001, article 6.2

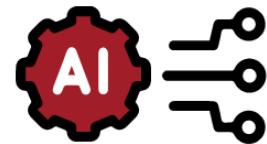
*L'organisme doit établir des objectifs d'IA pour les fonctions et niveaux concernés.*

*Les objectifs d'IA doivent:*

- a) être cohérents avec la politique d'IA;
- b) être mesurables (si possible);
- c) prendre en compte les exigences applicables;
- d) être surveillés;
- e) être communiqués;
- f) être mis à jour comme approprié;
- g) être tenus à jour sous la forme d'une information documentée.

*Lorsqu'il planifie la façon d'atteindre ses objectifs d'IA, l'organisme doit déterminer:*

- ce qui sera fait;
- quelles ressources seront requises;
- qui sera responsable;
- les échéances; et
- la façon dont les résultats seront évalués.



PECB

9

### **ISO/IEC42001, article6.2 Objectifs d'IA et plans pour les atteindre (suite)**

*NOTE Une liste non exhaustive des objectifs d'IA relatifs au management des risques figure à l'Annexe C. Les objectifs de mesure et les mesures permettant d'identifier les objectifs de développement et d'utilisation responsables des systèmes d'IA et les actions permettant de les atteindre sont spécifiés en A.6.1 et A.9.3 dans le tableauA.1. Les conseils de mise en œuvre de ces mesures figurent en B.6.1 et B.9.3.*

# Déterminer les objectifs du SMIA

Les objectifs liés à la mise en œuvre du SMIA peuvent être les suivants :

- Respecter les exigences légales, réglementaires et contractuelles liées à l'IA afin de garantir son utilisation responsable
- Faire preuve de diligence raisonnable dans la conception et l'exploitation des systèmes d'IA afin d'atténuer les risques et les responsabilités
- Inspirer confiance aux parties prenantes de l'organisme en matière de fiabilité et d'utilisation éthique des systèmes d'IA
- Améliorer la réponse de l'organisme aux incidents liés à l'IA, en minimisant l'impact potentiel des défaillances des systèmes d'IA ou des atteintes à la sécurité
- Réduire les coûts associés aux incidents liés à l'IA, y compris les coûts juridiques, financiers et de réputation
- Promouvoir l'innovation et le développement responsables de l'IA en adhérant à des principes et des lignes directrices éthiques en matière d'IA
- Encourager une culture de l'éthique et de la conformité en matière d'IA dans l'ensemble de l'organisme afin d'assurer des pratiques d'IA responsables à tous les niveaux
- Surveiller et évaluer en continu les performances des systèmes d'IA et les comportements éthiques, en procédant aux ajustements nécessaires pour maintenir les normes les plus élevées en matière de fiabilité et d'intégrité de l'IA

### 1.3.3 Déterminer le périmètre préliminaire

Pour déterminer le périmètre d'un SMIA, il convient qu'un organisme tienne compte des facteurs suivants :

- **Mandats et obligations** : Déterminer les mandats internes de l'organisme en matière de management de l'IA et les obligations externes liées aux systèmes d'IA.
- **Responsabilité du management** : Déterminer si la responsabilité du SMIA proposé relève de la responsabilité de plusieurs équipes de management, telles que différentes filiales ou différents départements.
- **Communication et documentation** : Définir la communication des documents relatifs au SMIA au sein de l'organisme, que ce soit par des moyens traditionnels comme le papier ou par des canaux numériques comme l'intranet.
- **Capacités du système** : Évaluer si le système de management actuel peut répondre de manière adéquate aux besoins de l'organisme en matière d'IA, y compris en termes d'efficacité opérationnelle, de maintenance et de fonctionnalité.

Pour déterminer le périmètre d'un SMIA, un organisme peut suivre les étapes suivantes :

- **Déterminer le périmètre préliminaire** : Cette activité devrait être menée par un groupe restreint, mais représentatif de la direction de l'organisme.
- **Déterminer le périmètre amélioré** : Les unités fonctionnelles à l'intérieur et à l'extérieur du périmètre préliminaire devraient être revues et soigneusement sélectionnées, afin de réduire le nombre d'interfaces le long des limites. Toutes les fonctions essentielles qui soutiennent l'activité devraient être prises en compte lors de l'amélioration du périmètre préliminaire.
- **Déterminer le périmètre final** : Le périmètre amélioré devrait être évalué, ajusté et expliqué avec précision par la direction de l'organisme.

**PECB** 11  
Approuver le périmètre : L'information documentée décrivant le périmètre devrait être approuvée par la direction.

Il convient que l'organisme prenne également en compte les activités qui ont un impact sur le SMIA, qu'elles soient menées en interne ou externalisées vers d'autres parties de l'organisme ou vers des fournisseurs indépendants. L'organisme devrait aussi identifier les interfaces, y compris les aspects physiques, techniques et organisationnels, et leur impact sur le périmètre du SMIA.

## 1.3.4 Analyser l'environnement interne et externe

### Avis pratiques

- La norme ISO/IEC 42001 ne propose pas d'approche pratique expliquant comment analyser le contexte d'un organisme. Les organismes sont donc libres de choisir l'approche qu'ils jugent la plus appropriée à leur contexte.
- Il existe de nombreuses approches qui aident à comprendre le fonctionnement d'un organisme. Lors de l'adoption d'une approche, l'important est d'identifier les caractéristiques des facteurs internes et externes qui influencent la mission d'un organisme, ses principales activités, les parties intéressées, etc.

P Politique

E Économique

S Social

T Technologique

### Environnement externe

Micro-environnement

Macro-environnement

S Strengths (Forces)

O Opportunities (Opportunités)

W Weaknesses (Faiblesses)

T Threats (Menaces)

S  
W  
O  
T

PECB

12

Plusieurs approches ont déjà été élaborées pour aider à analyser et à comprendre le contexte d'un organisme. Dans la plupart des organismes, des études de contexte ont été menées en interne ou auprès d'autres organismes. Il est conseillé de recueillir ces études, de les analyser et d'interviewer quelques acteurs clés pour s'assurer d'une bonne compréhension du contexte de l'organisme. Cependant, il est important de mentionner que ce processus ne représente pas un projet en soi.

Les approches suivantes sont particulièrement utiles pour analyser le contexte d'un organisme :

**Analyse SWOT:** L'analyse SWOT est utilisée pour effectuer une analyse approfondie des forces, des faiblesses, des opportunités et des menaces d'un organisme. L'analyse est effectuée dans le but de déterminer où l'organisme devrait investir ses ressources (tirer parti des opportunités, réduire les faiblesses, faire face aux menaces, etc.). Les forces et les faiblesses visent à évaluer les enjeux internes, tandis que les opportunités et les menaces servent à évaluer les enjeux externes d'un organisme.

**Analyse PEST (politique, économique, sociale et technologique):** L'analyse PEST permet à l'organisme d'analyser les forces du marché et les opportunités dans les quatre domaines suivants: social, technologique, économique et politique. Certains auteurs ont ajouté deux catégories supplémentaires: environnementale et légale.

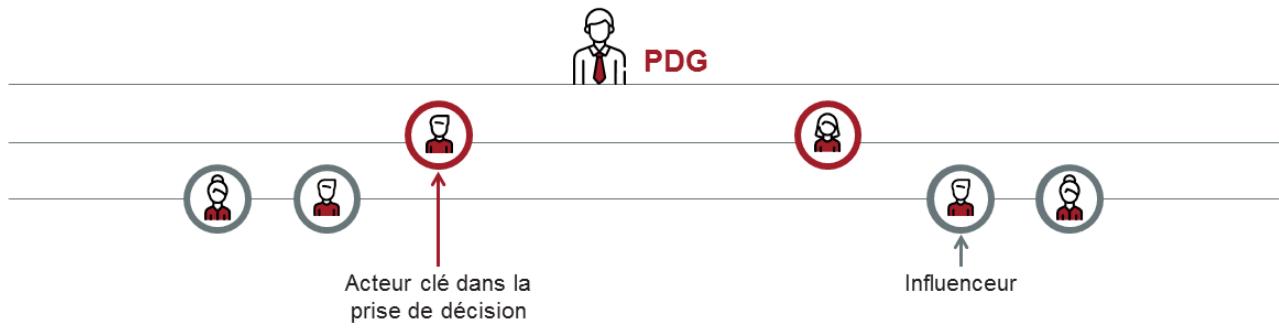
**L'analyse des cinq forces de Porter:** L'analyse des cinq forces de Porter examine le niveau de compétitivité d'un organisme en utilisant les cinq facteurs qui influencent l'environnement commercial au sein d'une industrie. Ces cinq forces sont l'intensité de la rivalité entre les concurrents, le pouvoir de négociation des clients, la menace des entrants potentiels sur le marché, le pouvoir de négociation des fournisseurs et la menace des produits ou services alternatifs.

# Analyser l'environnement interne et externe

## Structure organisationnelle et acteurs principaux

Afin de comprendre la structure et les principaux acteurs de l'organisme en termes de périmètre, il convient d'examiner les trois niveaux organisationnels suivants :

- **Stratégiques** (Qui définit les orientations stratégiques ?)
- **Du pilotage** (Qui coordonne et gère les opérations ?)
- **Opérationnels** (Qui participe aux opérations et aux autres activités de soutien ?)



PECB

13

Dans l'analyse du contexte interne d'un organisme, il est nécessaire d'identifier les structures regroupant les différents acteurs et les relations au sein de l'organisme (hiérarchiques et fonctionnelles). Il s'agit notamment de la séparation des tâches, des responsabilités, des autorités et de la communication au sein de l'organisme. Il convient également d'identifier les fonctions externalisées aux sous-traitants. La structure de l'organisme peut être de différents types :

1. **La structure divisionnaire:** Chaque division est placée sous l'autorité d'un directeur de division responsable des décisions stratégiques, administratives et opérationnelles au sein de cette unité.
2. **La structure fonctionnelle:** L'autorité fonctionnelle est exercée sur les procédures, y compris la planification et la prise de décision.

### Notes:

- Une division au sein de l'organisme peut être organisée en structures fonctionnelles et inversement.
- Un organisme peut avoir une structure matricielle lorsque l'ensemble de l'organisme est basé sur les deux types de structure (divisionnaire et fonctionnelle).
- Quelle que soit la structure, les niveaux suivants sont distingués:
  1. Le niveau stratégique (responsable des politiques et des stratégies)
  2. Le niveau de pilotage (responsable de la coordination et de la gestion des activités)
  3. Le niveau opérationnel (responsable de l'élimination des menaces et de la réduction des menaces et des risques liés à l'IA)

Les autres outils utilisés pour analyser le contexte interne d'un organisme incluent entre autres les suivants:

- Grille d'évaluation des capacités
- Modèle 7S de McKinsey
- Enquête appréciative
- Technique des compétences de base
- Analyse de portefeuille

# Enjeux internes et externes

## ISO/IEC 42001, article 4.1

*L'organisme doit déterminer les enjeux externes et internes pertinents compte tenu de sa mission et qui ont une incidence sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son système de management de l'IA.*

*NOTE 2 Les enjeux externes et internes à traiter au titre du présent article peuvent varier en fonction des rôles et des compétences de l'organisme et de leur impact sur sa capacité à atteindre le(s) résultat(s) attendu(s) de son système de management de l'IA. Ils peuvent inclure, mais ne sont pas limités à:*

*a) des considérations liées au contexte externe, telles que:*

- 1) les exigences légales applicables, y compris les utilisations interdites de l'IA;*
- 2) les politiques, lignes directrices et décisions des régulateurs qui ont un impact sur l'interprétation ou l'application des exigences légales en matière de développement et d'utilisation de systèmes d'IA;*
- 3) les incitations ou les conséquences associées à la finalité visée et à l'utilisation des systèmes d'IA;*
- 4) la culture, les traditions, les valeurs, les normes et l'éthique en matière de développement et d'utilisation de l'IA;*
- 5) le paysage concurrentiel et les tendances en matière de nouveaux produits et services utilisant des systèmes d'IA;*

*b) des considérations liées au contexte interne, telles que:*

- 1) le contexte organisationnel, la gouvernance, les objectifs, les politiques et les procédures;*
- 2) les obligations contractuelles et;*
- 3) la finalité visée par le système d'IA à développer ou à utiliser.*

PECB

14

# Contexte interne – Aspects principaux

## ISO/IEC 27000, article 3.38

*Environnement interne dans lequel l'organisme cherche à atteindre ses objectifs*

*Note 1 à l'article : Le contexte interne peut inclure:*

- la gouvernance, la structure organisationnelle, les rôles et les responsabilités;
- les politiques, objectifs et stratégies mises en place pour atteindre ces derniers;
- les capacités, en termes de ressources et de connaissances (par exemple: capital, temps, personnel, processus, systèmes et technologies);
- les systèmes d'information, flux d'information et processus de prise de décision (formels et informels);
- les relations avec les parties prenantes internes, les perceptions et valeurs associées à celles-ci;
- la culture de l'organisme;
- les normes, les lignes directrices et les modèles adoptés par l'organisme;
- la forme et l'étendue des relations contractuelles.

PECB

15

## 1.3.5 Identifier les processus et activités clés

### Activités de l'organisme

Quels sont les biens et les services produits par l'organisme ?

### Actifs

Quels sont les principaux actifs de l'organisme ?

### Processus opérationnels

Quels sont les principaux processus qui permettent à l'organisme de réaliser sa mission ?

**Note :** À cette étape, il ne s'agit pas d'effectuer une cartographie complète des processus, mais seulement d'établir une liste générale.

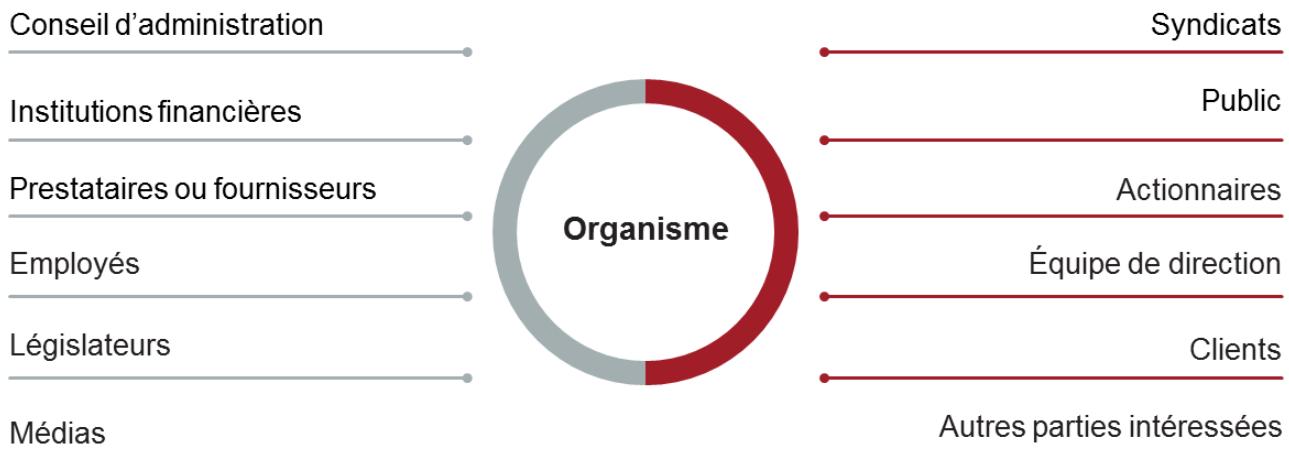
PECB

16

Il est essentiel que le chef de projet SMIA connaisse les activités de l'organisme qui ont une incidence sur le management de l'IA. En effet, le type de produits et services d'IA offerts par l'organisme aura une influence majeure sur son modèle opérationnel. Ces produits et services d'IA peuvent également exposer l'organisme à des risques particuliers, tels que la sécurité de l'information et les considérations éthiques.

Le chef de projet du SMIA devrait également connaître les processus opérationnels de l'organisme, car ceux-ci exposent l'organisme à de nombreux risques spécifiques à l'IA. À cet effet, il convient que le chef de projet analyse et comprenne la nature de ces processus et détermine les risques directs et indirects liés à l'IA auxquels l'organisme est exposé au cours de ses activités et processus.

## 1.3.6 Identifier et analyser les parties intéressées



**Note :** Le terme « partie intéressée » est synonyme de « partie prenante. » Par conséquent, ces termes sont utilisés de manière interchangeable.

PECB

17

### Définitions

#### **ISO9000, article3.2.3 Partie intéressée**

##### **partie prenante**

Personne ou organisme qui peut soit influer sur une décision ou une activité, soit être influencé ou s'estimer influencée par une décision ou une activité

**EXEMPLE** Clients, propriétaires, personnel d'un organisme, prestataires, établissements financiers, autorités réglementaires, syndicats, partenaires ou société qui peut inclure des concurrents ou des groupes de pression d'opposition.

**Note1 à l'article:** Il s'agit de l'un des termes communs et définitions de base pour les normes de systèmes de management de l'ISO, donnés dans l'Annexe SL du Supplément ISO consolidé aux Directives ISO/IEC, Partie 1. La définition initiale a été modifiée par l'ajout de l'Exemple.

#### **ISO9000, article3.2.4 Client**

Personne ou organisme qui est susceptible de recevoir ou qui reçoit un produit ou un service destiné à, ou demandé par, cette personne ou cet organisme

**EXEMPLE** Consommateur, utilisateur final, détaillant, destinataire d'un produit ou service issu d'un processus interne, bénéficiaire et acheteur.

**Note1 à l'article:** Le client peut être interne ou externe à l'organisme.

#### **ISO9000, article3.2.5. Prestataire**

##### **Fournisseur**

Organisme qui procure un produit ou un service

**EXEMPLE** Producteur, distributeur, détaillant ou marchand d'un produit ou d'un service.

**Note1 à l'article:** Un prestataire peut être interne ou externe à l'organisme.

Licensed to Quesnot Xavier (xavier@getcaas.io)

©Copyrighted material PECB®. Single user license only, copying and networking prohibited. Downloaded: 2025-03-31

*Note 2 à l'article: Dans une situation contractuelle, le prestataire peut être appelé «contractant».*

# Page de notes

---

PECB

18

L'identification et l'analyse des parties intéressées peuvent s'avérer difficiles en raison des nombreuses questions qui peuvent se poser, y compris les questions conceptuelles, telles que le traitement des différences culturelles ou procédurales:

- Comment approcher les parties intéressées et comment les gérer à long terme
- Comment équilibrer les différents avis et besoins des parties intéressées
- Comment classer les parties intéressées lorsqu'il n'y a pas de frontières claires entre elles, lorsqu'il existe plusieurs groupes de parties intéressées ou lorsqu'il y a une forte coalition évidente entre certains groupes

## ***ISO/IEC42001, article4.1 Compréhension de l'organisme et de son contexte***

*NOTE1 Pour comprendre l'organisme et son contexte, il peut être utile que l'organisme détermine les rôles relatifs au système d'IA. Ces rôles peuvent inclure, sans toutefois s'y limiter, un ou plusieurs des acteurs suivants:*

- *fournisseurs d'IA, y compris les fournisseurs de plateformes d'IA, les fournisseurs de produits ou de services d'IA;*
- *producteurs d'IA, y compris les développeurs d'IA, les concepteurs d'IA, les opérateurs d'IA, les testeurs et évaluateurs d'IA, les déployeurs d'IA, les professionnels des facteurs humains de l'IA, les experts de domaine, les évaluateurs d'impact de l'IA, les responsables d'achat, les professionnels de la gouvernance et de la surveillance de l'IA;*
- *les clients de l'IA, y compris les utilisateurs de l'IA;*
- *les partenaires de l'IA, y compris les intégrateurs de systèmes d'IA et les fournisseurs de données;*
- *les sujets de l'IA, y compris les sujets des données et d'autres sujets; et*
- *les autorités compétentes, y compris les décideurs politiques et les régulateurs.*

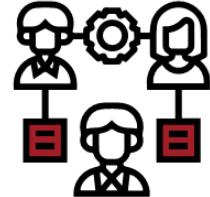
*La norme ISO/IEC22989 fournit une description détaillée de ces rôles. En outre, les types de rôles et leur relation avec le cycle de vie du système d'IA sont également décrits dans le cadre de management des risques de l'IA du NIST. Les rôles de l'organisme peuvent déterminer l'applicabilité et l'étendue de l'applicabilité des exigences et des mesures figurant dans le présent document.*

# Besoins et attentes des parties intéressées

## ISO/IEC 42001, article 4.2

*L'organisme doit déterminer:*

- les parties intéressées concernées par le système de management de l'IA;
- les exigences pertinentes de ces parties intéressées;
- lesquelles de ces exigences seront prises en compte par le système de management de l'IA.



*NOTE Les parties intéressées pertinentes peuvent avoir des exigences liées au changement climatique.*

**PECB**

19

# Analyser les exigences et les attentes des parties intéressées

L'identification et l'analyse des parties intéressées peuvent se faire de la manière suivante :

## 1. Identifier leurs exigences et leurs attentes

- Il convient que les organismes identifient les exigences et les attentes des parties intéressées, qui peuvent être implicites ou explicites.
- **Exemple :** Un taux de disponibilité du service de 95 %.

## 2. Valider leurs exigences et leurs attentes

- Les organismes devraient ensuite valider les exigences et les attentes des parties intéressées, notamment en analysant si ces exigences et ces attentes répondent et sont liées au contexte de l'organisme et aux enjeux auxquels il est confronté à ce moment-là.

## 3. Définir leurs rôles et responsabilités

- Afin de faciliter le processus de mise en œuvre, il est important que les organismes informent leurs parties intéressées des rôles, des responsabilités et de la participation qu'elles auront dans le processus de mise en œuvre. Il convient généralement de le faire avant le processus de mise en œuvre, afin que les parties intéressées soient pleinement conscientes de leurs responsabilités et les comprennent.

PECB

20

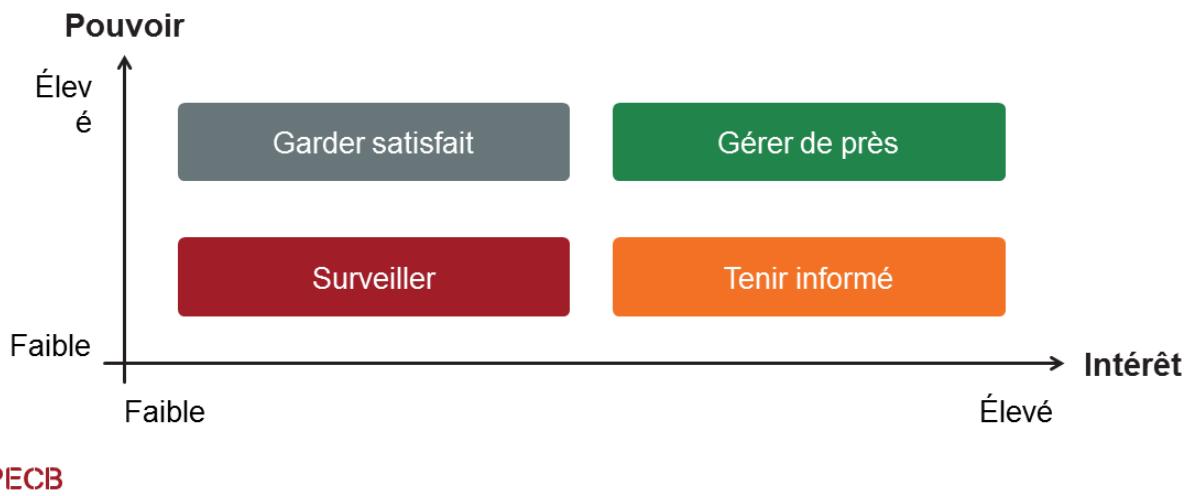
William C. Frederick, James E. Post et Keith Davis écrivent dans leur livre *Business and Society: Corporate Strategy, Public Policy, Ethics* que l'analyse des parties intéressées comporte les six étapes suivantes<sup>[1]</sup>:

1. Cartographier les relations entre les parties intéressées
2. Cartographier les coalitions des parties intéressées
3. Évaluer la nature de l'intérêt de chaque partie prenante
4. Évaluer la nature du pouvoir de chaque partie prenante
5. Construire une matrice des priorités des parties prenantes
6. Surveiller les coalitions changeantes

**Note:** L'organisme est tenu d'informer toutes les parties intéressées des mesures prises concernant le SMIA, ainsi que de l'impact et des responsabilités qu'elles y assument.

# Matrice pouvoir/intérêt des parties intéressées

La matrice pouvoir/intérêt, élaborée par Johnson et Scholes, est un outil qui aide à déterminer et à gérer les parties intéressées. [2]

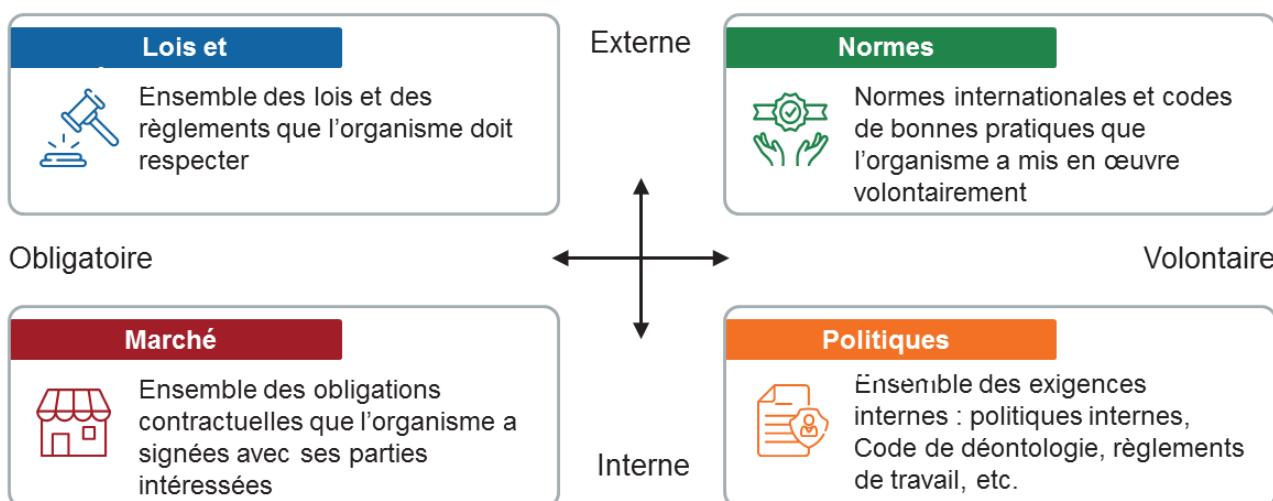


La matrice illustrée dans la diapositive montre la relation entre deux variables importantes (intérêt et pouvoir). D'une part, la variable d'intérêt montre l'intérêt des parties intéressées pour les décisions et les activités de l'organisme. D'autre part, la variable de pouvoir montre le degré de pouvoir des parties intéressées sur les décisions et les activités de l'organisme. Grâce à cette matrice, les organismes peuvent prioriser les efforts nécessaires pour répondre aux exigences et aux attentes des parties intéressées. [2]

Les organismes peuvent également catégoriser les différentes parties intéressées dans la matrice en fonction des priorités suivantes[2] :

- Identifier et répertorier les parties intéressées pertinentes
- Déterminer les besoins et les attentes des parties intéressées en utilisant différentes méthodes de recherche
- Classer les parties intéressées en fonction du pouvoir et de l'intérêt
- Établir des priorités et des objectifs et réduire le risque de ne pas répondre aux exigences et aux attentes

## 1.3.7 Identifier et analyser les exigences métier



PECB

22

L'organisme doit tenir compte des exigences commerciales, légales ou réglementaires, de même que des obligations contractuelles qu'il a conclues avec les parties intéressées. Pour ce faire, il est important d'identifier et de prendre en compte toutes les exigences de l'organisme qui pourraient impacter la mise en œuvre du SMIA. Elles doivent être incluses dans l'appréciation du risque selon laquelle le risque de non-conformité est analysé. Il est à noter que, pour l'identification et l'analyse des exigences légales et contractuelles, il convient d'impliquer des conseillers juridiques ou des juristes qualifiés dans le domaine. Un expert en management de l'intelligence artificielle n'est généralement pas apte, par exemple, à analyser les implications juridiques et, par conséquent, peut ne pas identifier les exigences légales et contractuelles.

Les exigences de management de l'IA pour tous les organismes sont principalement déterminées par quatre sources:

- Lois et règlements:** Ces sources seront abordées dans la diapositive suivante.
- Normes:** Les organismes doivent se conformer à un ensemble de normes internationales et de codes de pratique liés à leur secteur d'activité. Bien que la mise en œuvre des cadres réglementaires soit volontaire, ils deviennent des obligations à respecter (avec le risque de perdre sa certification en cas de défaut grave), du point de vue du management de l'intelligence artificielle.
- Marché:** Les exigences de marché comprennent l'ensemble des obligations contractuelles que l'organisme a signées avec ses parties prenantes. Un manquement aux obligations contractuelles peut entraîner des pénalités (lorsque cela est prévu dans les contrats) ou des poursuites civiles pour préjudices subis. Les exigences de marché sont toutes des règles implicites qu'un organisme devrait respecter pour mener ses activités. Par exemple, bien qu'un organisme n'ait pas d'obligation contractuelle de livrer ses produits comme prévu, il va de soi qu'il s'agit d'une politique commerciale pour respecter les délais de livraison prévus et que le non-respect de cette obligation entraînera une perte de parts de marché, une perte de confiance des clients, de bénéfices, etc.
- Politiques internes:** Les politiques internes constituent des principes, des règles et des lignes directrices qui comprennent toutes les exigences définies au sein de l'organisme: politiques internes, codes éthiques, conditions de travail, etc. Il est à noter que le non-respect des politiques internes n'a pas nécessairement d'implications juridiques.

# Comprendre les exigences légales et s'y conformer

## Appréciation et classification des risques

Le cadre réglementaire proposé par l'UE pour l'IA définit des règles et des obligations spécifiques pour les systèmes d'IA, en les classant en fonction des niveaux de risque. Bien que l'adoption de la norme ISO/IEC 42001 ne soit pas une obligation légale, les organismes, en appliquant cette norme, s'alignent sur ces exigences légales à travers l'appréciation complète des risques liés à l'IA. Cette démarche s'aligne sur la catégorisation de l'UE basée sur les risques, garantissant que le système de management de l'IA traite et atténue les risques.

## Transparence et redevabilité

Le cadre réglementaire proposé par l'UE pour l'IA souligne la nécessité de transparence et de traçabilité des systèmes d'IA. La mise en œuvre de la norme ISO/IEC 42001 facilite la mise en place de processus solides pour une utilisation, une conception, un développement et un fonctionnement responsables des systèmes d'IA. Elle garantit que les organismes respectent les attentes légales, favorisant la transparence et la redevabilité tout au long du cycle de vie de l'IA.

PECB

23

Le cadre réglementaire proposé par l'UE pour l'IA identifie les systèmes d'IA inacceptables et à haut risque, en précisant les cas où certaines applications d'IA sont interdites ou autorisées avec des restrictions. En mettant en œuvre la norme ISO/IEC42001, les organismes prennent en compte les considérations éthiques dans l'utilisation, la conception, le développement et le déploiement de l'IA, s'alignant ainsi sur ces exigences légales.

Les organismes doivent se conformer aux lois et réglementations applicables pour garantir le développement et le déploiement responsables des systèmes d'IA. Le non-respect de ces exigences légales peut avoir des conséquences juridiques, entraîner des sanctions financières et nuire à la réputation d'un organisme.

# Résumé de la section :

- Pour comprendre un organisme et son contexte, il est nécessaire d'obtenir des informations générales sur sa mission, ses stratégies, sa finalité et ses valeurs. L'alignement des objectifs du SMIA sur la mission de l'organisme peut être ainsi assuré.
- La structure de l'organisme peut être divisionnaire et fonctionnelle.
- L'organisme doit se conformer aux lois et règlements appropriés.
- Pour identifier et analyser les parties intéressées, l'organisme utilise un certain nombre d'outils, tels que l'identification et la validation de leurs exigences et attentes, la définition de leurs rôles et responsabilités.
- Les exigences du SMIA pour tous les organismes proviennent de quatre sources : les lois et règlements, le marché, les politiques internes et les normes.



Questions ?



Quizz 7

PECB

24

**Note:**Pour répondre au Quizz7, veuillez accéder à la fiche Quizz.

# Section 9

## Périmètre du SMIA

- Limites du SMIA
- Limites organisationnelles
- Limites du système d'information
- Limites physiques
- Déclaration du périmètre du SMIA

PECB

25

Cette section fournit des informations qui aideront le participant à acquérir des connaissances sur les éléments clés du périmètre du SMIA, couvrant les limites organisationnelles, les limites du système d'information et les limites physiques, ainsi que l'importance de la déclaration de périmètre du SMIA.

# Périmètre du SMIA

## 1. Définir et établir

- 1.1 Leadership et approbation du projet
- 1.2 Rôles et responsabilités
- 1.3 L'organisme et son contexte
- 1.4 Périmètre du SMIA**
- 1.5 Analyse du système existant
- 1.6 Politique d'IA
- 1.7 Management du risque lié à l'IA
- 1.8 Déclaration d'applicabilité

## 2. Mettre en œuvre et opérer

- 2.1 Sélection et conception des mesures
- 2.2 Mise en œuvre des mesures
- 2.3 Gestion des informations documentées
- 2.4 Communication
- 2.5 Compétence et sensibilisation
- 2.6 Gestion des opérations d'IA

## 3. Surveiller et revoir

- 3.1 Surveillance, mesurage, analyse et évaluation
- 3.2 Audit interne
- 3.3 Revue de direction

## 4. Maintenir et améliorer

- 4.1 Traitement des non-conformités
- 4.2 Amélioration continue

PECB

26

# Exigences d'ISO/IEC 42001 en termes de périmètre du SMIA

## ISO/IEC 42001, article 4.3

*Pour établir le périmètre du système de management de l'IA, l'organisme doit en déterminer ses limites et son applicabilité.*

*Lorsque l'organisme établit ce périmètre, il doit prendre en compte:*

- les enjeux externes et internes auxquels il est fait référence en 4.1;*
- les exigences auxquelles il est fait référence en 4.2.*

*Le périmètre doit être disponible sous la forme d'une information documentée.*

*Le périmètre du système de management de l'IA doit déterminer les activités de l'organisme en vue de satisfaire les exigences du présent document en termes de système de management de l'IA, de leadership, de planification, de soutien, de fonctionnement, de performances, d'évaluation, d'amélioration, de mesures et d'objectifs.*

**PECB**

27

# Périmètre

## Importance

Une définition claire du périmètre est un facteur de réussite important pour la mise en œuvre du SMIA. Il permet de faciliter les résultats suivants :

- Obtenir le soutien de la direction
- Mobiliser les parties intéressées pour le projet
- Justifier une plus-value aux parties intéressées

**Note :** La définition du périmètre est une activité clé qui pose les fondements essentiels des autres activités de mise en œuvre du SMIA.

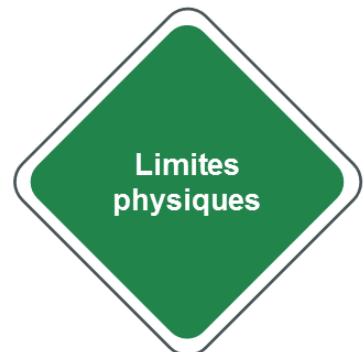
PECB

28

Lorsque l'organisme dispose déjà d'un système de management, tel qu'un système de management de la qualité (SMQ) conformément à la norme ISO9001, le périmètre du SMIA peut soit chevaucher partiellement le système existant, soit fonctionner indépendamment de celui-ci.

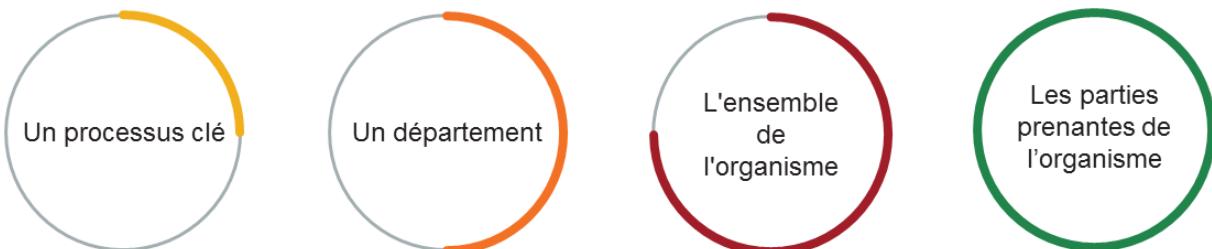
# Limites du SMIA

Trois dimensions sont à prendre en compte pour définir les limites du périmètre du SMIA :



# Limites organisationnelles

Les limites organisationnelles du périmètre peuvent inclure :



PECB

30

Deux approches de la définition du terme «limite» sont généralement contraignantes. L'approche réaliste adoptera la définition de limite employée par les utilisateurs eux-mêmes. En revanche, selon une approche commune, le responsable du programme choisira une limite qui atteint ses objectifs analytiques. Les limites géographiques (bureau de l'entreprise, etc.) et temporelles (temps, programmes de bureau) sont des méthodes pratiques pour définir les limites organisationnelles d'un organisme.

Pour définir les limites organisationnelles, les éléments suivants doivent être pris en compte:

1. Unités organisationnelles: départements, projets de service, filiales, etc.
2. Structures organisationnelles et responsabilités des managers
3. Processus opérationnels: ventes, achats, etc.

Une méthode efficace pour définir les limites organisationnelles est d'analyser les responsabilités et les zones d'influence des principaux décideurs de l'organisme. Par exemple, si un organisme planifie de mettre en œuvre un SMIA dans son département de recherche et développement IA, en analysant les principaux processus et services qui relèvent du directeur de ce département, les limites peuvent être proposées au niveau organisationnel. Par conséquent, si le déploiement du modèle est géré par le département informatique (plutôt que par le département de recherche et développement de l'IA), cette responsabilité doit être documentée comme étant exclue du périmètre.

Les livrables pour cette activité sont :

1. Description des limites organisationnelles avec justification documentée des exceptions
2. Description des structures organisationnelles incluses dans le SMIA
3. Identification des processus opérationnels et des actifs informationnels (avec leurs propriétaires) liés à l'IA
4. Identification de «l'orientation et des processus décisionnels».

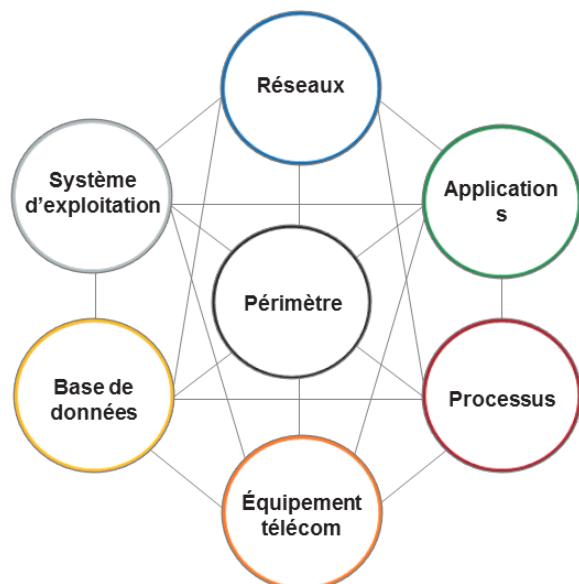
**Note:** Si un organisme est très décentralisé en termes de prise de décision, il peut être souhaitable de mettre en place un SMIA différent pour chaque division et de les faire ensuite certifier chacun de façon indépendante. Au contraire, un organisme très centralisé aura plutôt tendance à vouloir ne disposer que d'un SMIA dirigé et contrôlé à partir du siège social.

# Limites du système d'information

Tous les composants du système doivent être pris en compte ; l'accent ne doit pas être mis uniquement sur les composants matériels.

**Note :** En théorie, l'absence d'infrastructure technique n'empêche pas un organisme d'obtenir une certification ISO/IEC 42001.

PECB



31

Pour ce qui est des limites des systèmes d'information, l'ensemble des éléments des systèmes devrait être pris en considération, et non se limiter aux éléments matériels tels que les serveurs et l'équipement de télécommunication. Il faut également considérer les contraintes technologiques et les obligations contractuelles de l'organisme.

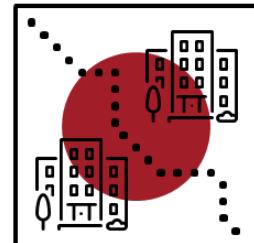
Les limites des systèmes d'information se définissent notamment en termes de :

1. Réseaux : réseaux internes, réseaux sans fil, etc.
2. Systèmes d'exploitation: Windows, Linux, etc.
3. Applications : CRM (customer relationship management), logiciel de gestion de paie, ERP (enterprise resource planning), utilitaires, base de données
4. Base de données : fichiers clients, données médicales, recherche et développement, etc.
5. Processus : considérer les processus qui transportent, entreposent ou traitent l'information
6. Équipements de télécommunication : routeurs, pare-feux, etc.

Les systèmes d'information supportant les processus opérationnels devraient être inclus dans les limites organisationnelles du périmètre. Par exemple, il serait inapproprié d'exclure les bases de données clients et le CRM du périmètre si celui-ci inclut la gestion des comptes clients et le département de service client. L'ensemble des activités d'un processus et l'échange d'informations inclus dans le périmètre, y compris les éléments d'entrée et de sortie, devraient être pris en considération. Par exemple, un organisme prévoit de faire certifier son service d'émission de chèque. À l'interne, un logiciel sert à la saisie des données et à transférer l'information à une tierce partie qui émet les chèques. L'organisme doit s'assurer de la sécurité de l'information, non seulement lors de la saisie en entrée, mais également lors de son transfert et de son traitement externalisé. Cette assurance pourrait par exemple prendre la forme d'un accord contractuel.

# Limites physiques

- L'ensemble des lieux physiques, autant internes qu'externes, inclus dans le SMIA, devrait être pris en considération.
- Ces sites comprennent tous les lieux situés dans le périmètre ou dans une partie du périmètre du SMIA et l'infrastructure physique nécessaire à leur fonctionnement.
- Dans le cas des sites loués, il est essentiel de tenir compte des interfaces avec le SMIA et des accords de service correspondants.



PECB

32

Les limites physiques d'un SMIA couvrent un large éventail de matériel et d'infrastructures, essentiels au bon fonctionnement et à la gestion des systèmes d'IA. Les systèmes d'IA reposent essentiellement sur du matériel avancé, tel que des serveurs, des processeurs à haute performance, tels que des GPU adaptés aux tâches d'apprentissage profond, des dispositifs de stockage de capacité suffisante et des équipements de réseau complets. Ces composants assurent le traitement et le stockage efficaces de grandes quantités de données. Les centres de données qui hébergent la puissance de calcul et les capacités de stockage nécessaires aux charges de travail exigeantes de l'IA repoussent encore ces limites. Ces centres sont équipés d'infrastructures critiques, notamment de systèmes d'alimentation électrique et de refroidissement, ainsi que de dispositifs de sécurité, afin d'assurer un fonctionnement ininterrompu du matériel.

De plus, le périmètre physique d'un SMIA comprend des dispositifs informatiques périphériques tels que des appareils IoT, des smartphones et des serveurs périphériques, qui permettent le prétraitement des données à la source afin de minimiser la latence et la consommation de bande passante. L'infrastructure de mise en réseau comble le fossé entre les composants disparates du système, qu'ils soient situés dans une seule installation ou répartis dans le monde entier, en assurant une transmission transparente des données par le biais de routeurs, de commutateurs et d'une connectivité internet robuste. Les systèmes de sécurité font partie intégrante de l'infrastructure, protégeant le matériel et les données contre les accès non autorisés ou les dommages grâce à des mesures telles que la surveillance, les contrôles biométriques et les enceintes sécurisées pour les serveurs. Dans certains cas, les systèmes de management de l'IA sont interconnectés avec des systèmes physiques, par exemple, dans la fabrication ou les véhicules autonomes, l'IA est combinée avec des applications du monde réel. Il est donc nécessaire de définir les limites tangibles à l'intérieur desquelles l'IA opère, qui peuvent impacter à la fois le domaine numérique et le domaine physique.

# Déclaration de périmètre

Il convient que l'organisme prépare une déclaration définissant le périmètre du SMIA en fonction de la taille, de la nature et de la complexité de l'organisme. Cette déclaration devrait être mise à la disposition des parties intéressées.

La déclaration de périmètre devrait être :

- Aussi simple que possible
- Compréhensible par les parties externes et celles ayant une connaissance limitée de l'organisme
- Suffisamment précise pour montrer ce qui est couvert par le SMIA, si l'organisme souhaite s'engager dans un processus de certification formel.

**Note :** Le processus de définition du périmètre du SMIA est mené à bien au niveau de la direction ; des experts métiers tels que des consultants et des analystes d'affaires peuvent apporter leur aide.

# Modifications du périmètre

Le périmètre peut être modifié au fil du temps afin que le SMIA continue de contribuer à l'atteinte des objectifs de l'organisme en matière d'IA.

Des modifications de périmètre peuvent s'avérer nécessaires pour les raisons suivantes :

- Modifications dans l'environnement interne (réorganisation, nouveaux produits, services, méthodes de travail, processus, etc.)
- Modifications dans l'environnement externe (légal, concurrentiel, technologique)
- Émergence de nouveaux risques et de nouvelles opportunités
- Activités d'amélioration continue



Toute modification du périmètre doit être évaluée, approuvée et documentée.

# Résumé de la section :

- Une définition claire du périmètre est essentielle à la réussite de la mise en œuvre d'un SMIA.
- Trois types de limites d'un SMIA devraient être pris en compte : les limites organisationnelles, les limites du système d'information et les limites physiques.
- Le périmètre d'un SMIA peut varier considérablement d'une mise en œuvre à l'autre, englobant des processus, des fonctions, des services, des sections ou des sites spécifiques, des entités juridiques ou administratives entières, ainsi que leurs fournisseurs.
- Il convient que la déclaration du périmètre du SMIA soit réalisée au niveau de la direction ; des experts métiers tels que des consultants et des analystes d'affaires peuvent apporter leur aide.



Questions ?



Quiz 8

PECB

35

**Note:**Pour répondre au Quizz8, veuillez accéder à la fiche Quizz.

# Section 10

## Analyse du système existant

- Déterminer l'état actuel
- Effectuer une analyse des écarts
- Établir des objectifs de maturité
- Publier un rapport d'analyse des écarts

PECB

36

Cette section fournit des informations qui aideront les participants à comprendre le processus de réalisation d'une analyse des écarts et d'établissement des objectifs de maturité.

# Analyse du système existant

1. Définir et établir		2. Mettre en œuvre et opérer		3. Surveiller et revoir		4. Maintenir et améliorer	
1.1	Leadership et approbation du projet	2.1	Sélection et conception des mesures	3.1	Surveillance, mesurage, analyse et évaluation	4.1	Traitement des non-conformités
1.2	Rôles et responsabilités	2.2	Mise en œuvre des mesures	3.2	Audit interne	4.2	Amélioration continue
1.3	L'organisme et son contexte	2.3	Gestion des informations documentées	3.3	Revue de direction		
1.4	Périmètre du SMIA	2.4	Communication				
1.5	<b>Analyse du système existant</b>	2.5	Compétence et sensibilisation				
1.6	Politique d'IA	2.6	Gestion des opérations d'IA				
1.7	Management du risque lié à l'IA						
1.8	Déclaration d'applicabilité						

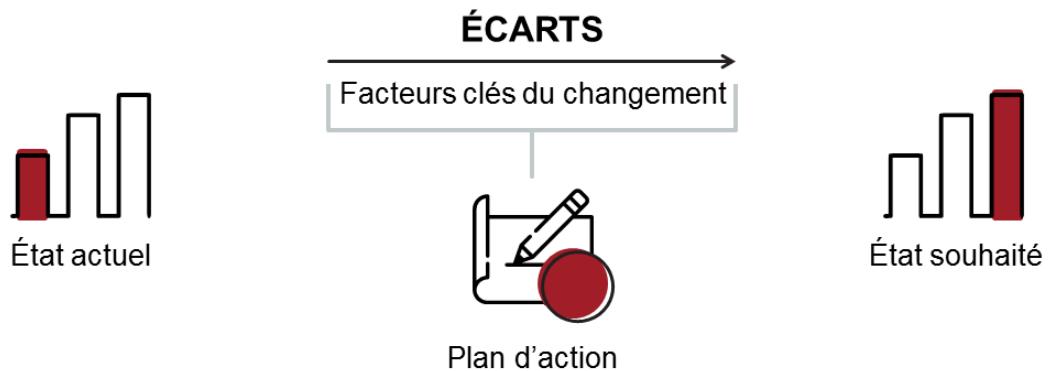
PECB

37

# Analyse des écarts

## Comprendre l'analyse des écarts

L'analyse des écarts est une technique permettant de déterminer les mesures à prendre pour passer d'un état actuel à un état futur souhaité.



PECB

38

L'analyse des écarts permet de déterminer l'état actuel, l'état souhaité et la différence entre les deux.

# 1.5 Analyse du système existant

## Liste des activités

1.5.1

Effectuer une analyse des écarts

1.5.3

Présenter le rapport d'analyse des écarts

1.5.2

Établir des objectifs de maturité

PECB

39

## 1.5.1 Effectuer une analyse des écarts

Une analyse des écarts se déroule comme suit :

1

Déterminer l'état actuel :

L'organisme a mis en place une routine pour la réalisation d'évaluations de l'impact du système d'IA. Toutefois, il n'existe actuellement aucun processus structuré permettant de documenter les résultats de ces évaluations.

2

Identifier les cibles (objectifs) :

Il convient d'affiner le SMIA afin d'intégrer un processus de documentation complet permettant d'enregistrer les résultats de toutes les évaluations d'impact du système d'IA.

3

Analyse des écarts :

Pour combler cette lacune, l'organisme doit établir et communiquer un protocole de documentation normalisé pour l'enregistrement des résultats des évaluations d'impact des systèmes d'IA. L'objectif est de s'aligner sur les exigences de la norme ISO/IEC 42001, en veillant à ce que les résultats de toutes les évaluations d'impact des systèmes d'IA soient documentés et conservés de manière cohérente.

PECB

40

Une analyse des écarts se déroule comme suit:

- **Déterminer l'état actuel:** Il convient d'identifier les processus et les mesures d'IA existants au sein d'un organisme.
- **Identifier l'état souhaité (objectifs):** Il convient de fixer les cibles de chaque mesure d'IA en les comparant à celles d'autres structures ou divisions au sein de l'organisme.
- **Effectuer l'analyse des écarts:** Il convient d'identifier l'écart pouvant exister entre les mesures de l'IA en place et les exigences de la norme ISO/IEC42001. Ceci permet à l'organisme de déterminer les mesures actuelles qui doivent être améliorées et de planifier en conséquence pour y remédier.

L'analyse des écarts aide à identifier et mesurer les investissements en temps, argent, ressources humaines et autres ressources pour une mise en œuvre efficace du SMIA.

# Déterminer l'état actuel

## La nécessité d'analyser le système de management existant

- La détermination de l'état actuel est une étape critique qui permet de comprendre où se situe l'organisme par rapport à ses objectifs.
- Cette phase implique une revue complète des opérations, des processus et des performances de l'organisme.
- Une analyse du système existant est nécessaire pour obtenir les connaissances adéquates et entreprendre les étapes nécessaires pour se conformer aux exigences de l'ISO/IEC 42001.

PECB

41

Pour obtenir une compréhension globale de la situation actuelle d'un organisme, les étapes suivantes peuvent être envisagées:

1. **Identifier les principales sources d'information:** Déterminer qui détient les informations nécessaires, qu'elles soient documentées ou qu'elles soient connues de personnes internes ou externes à l'organisme.
2. **Choisir les méthodes de collecte de données appropriées:** Choisir des méthodes adaptées au type d'informations nécessaires, en utilisant une combinaison d'approches qualitatives (par exemple, entretiens, groupes de discussion) et quantitatives (par exemple, analyse financière, enquêtes).
3. **Mener une analyse approfondie:** Collecter et analyser les données de façon systématique afin de comprendre les différentes facettes de l'état opérationnel, financier et organisationnel actuel.
4. **Documenter l'état actuel:** Organiser les résultats dans un format structuré, en énumérant clairement les processus, les flux de travail, les indicateurs de performance et les éclairages des parties prenantes.
5. **Évaluer en fonction des objectifs:** Évaluer comment l'état actuel s'aligne sur les objectifs de l'organisme, en identifiant les domaines d'alignement, de dépassement ou d'insuffisance.
6. **Identifier les écarts préliminaires:** Noter les domaines initiaux nécessitant une amélioration ou un ajustement sur la base de la comparaison entre les performances actuelles et les résultats souhaités.

# Collecte d'information



## Observations

Effectuer une observation des opérations de l'organisme, du système et du personnel impliqué afin de bien les comprendre



## Questionnaires

Envoyer un questionnaire à un échantillon de personnes qui sont représentatives des parties intéressées



## Entretiens

Mener des entretiens avec des personnes clés à différents niveaux hiérarchiques de l'organisme.



## Revue de la documentation

Lire et analyser les informations documentées pertinentes (par exemple, les politiques internes, les procédures, les rapports d'audit précédents, les contrats)



## Outils de diagnostic

Utiliser des outils techniques pour détecter des vulnérabilités techniques, établir une liste des actifs ayant un impact potentiel sur le réseau, effectuer une revue de code, etc.

PECB

42

Il convient que le chef de projet, en coopération avec l'équipe de projet, collecte des informations auprès de plusieurs parties intéressées afin de comprendre le système de management existant.

Pour déterminer l'état du système de management existant, le chef de projet tient compte de nombreux facteurs, tels que la méthode de collecte des données utilisée, les personnes à interroger, leurs compétences et leurs connaissances, la disponibilité des ressources (par exemple, en termes de budget et de temps).

Les actions suivantes peuvent contribuer à la collecte d'informations sur un organisme:

- Observer les processus et les contrôles (mesures) sur site de l'organisme en matière d'IA
- Mener des entretiens avec les personnes responsables de la gestion et des opérations quotidiennes du SMIA
- Revoir les informations documentées contenant les mesures d'IA (processus, procédures, description des contrôles, rapports).
- Consulter les rapports de l'audit interne

# Mener un entretien

Recommandations pour la réalisation des entretiens :

-  Utilisez des questions ouvertes et évitez les questions fermées ou guidées
-  S'assurer que tous les sujets sont couverts dans le temps imparti pour l'entretien
-  Prenez des notes durant l'entretien
-  Poser des questions pour clarifier une réponse ou une situation

PECB

43

La préparation est l'un des éléments clés pour mener à bien un entretien productif. Une stratégie efficace peut consister à créer des listes de contrôle qui assurent la conduite systématique des entretiens et l'obtention d'informations pertinentes. Les listes de contrôle devraient comporter une section pour les réponses, les commentaires et les observations, ainsi que des références à des normes connexes, le cas échéant.

Lors des entretiens, il peut être utile de clarifier la terminologie spécialisée liée au SMIA dans un langage plus compréhensible pour les personnes interrogées.

L'entretien peut être enregistré si la personne l'accepte. Cependant, la pratique la plus commune est simplement de prendre des notes. L'enregistrement de l'entretien peut être interprété comme intimidant par la personne interrogée et cela pourrait avoir un impact négatif sur les résultats de l'entretien.

**Les notes d'entretien devraient contenir les éléments suivants:**

- Fonction de la personne interrogée et date (en raison du principe de confidentialité, le nom de la personne interrogée ne figure pas dans les notes d'entretien, sauf s'il s'agit d'un membre de la direction).
  - Exemple: Discussion avec un employé du service informatique, le 20janvier 2024
- Objectifs de l'entretien
  - Exemple: Valider si l'organisme a organisé des formations conformément à sa politique
- Résumé des preuves collectées (les informations documentées devraient être collectées dans un langage clair, concis et précis; seuls les faits, et non les jugements, devraient être inclus; tous les points faibles devraient être identifiés et signalés dans l'analyse des écarts; la référence à la norme correspondante devrait être indiquée avec le numéro de l'article).

# Entretiens individuels et de groupe



## Individuels

Les entretiens individuels fournissent généralement des informations plus précises et permettent une appréciation plus approfondie du SMIA.

## Entretien s



## De

## groupe

Les entretiens de groupe sont plus efficaces pour établir les critères de base afin de parvenir à un consensus sur l'analyse du SMIA.

PECB

44

Toutes les parties intéressées, qu'il s'agisse d'experts ou non, devraient être interrogées sur leurs activités et leurs tâches afin d'obtenir des informations sur les risques liés à l'IA dans leur domaine. Les personnes responsables des processus métier fourniront une vision beaucoup plus «opérationnelle» des risques; par exemple, le responsable des relations publiques indiquera ses préoccupations concernant le risque pour la réputation.

### Entretiens individuels :

L'avantage le plus important des entretiens individuels est le fait de n'interroger qu'une seule personne à la fois pour permettre à l'enquêteur d'obtenir des informations plus détaillées sur le SMIA. De cette manière, l'enquêteur peut obtenir une compréhension plus complète de l'organisme et de son SMIA. L'enquêteur est en mesure de lire le langage corporel de la personne interrogée et peut demander des explications supplémentaires sur les réponses. Toutefois, la durée de l'entretien peut prendre beaucoup de temps si le nombre de personnes à interroger est élevé.

### Entretiens de groupe :

Les entretiens de groupe sont utiles lorsque le temps manque pour mener des entretiens individuels ou lorsque l'enquêteur souhaite examiner l'interaction entre les membres du groupe. Cependant, les entretiens de groupe peuvent produire des réponses biaisées, car un membre dominant du groupe peut influencer la réponse des autres par ce que l'on appelle «l'effet d'entraînement.»

# Questionnaires

## Questions ouvertes et fermées

### Exemples de questions ouvertes :

- 1 Comment améliorerez-vous la mise en œuvre du SMIA ?
- 2 Quels outils ont été utilisés pour mesurer l'efficacité de la mise en œuvre du SMIA ?
- 3 Pouvez-vous mentionner et expliquer l'approche que vous avez adoptée pour définir les rôles et les responsabilités du SMIA ?
- 4 Quels sont les points sur lesquels vous vous êtes concentré lors de la session de formation ?
- 5 En l'absence d'un SMIA, comment l'organisme évalue-t-il et surveille-t-il actuellement les risques potentiels liés aux systèmes d'IA ?
- 6 En l'absence d'un SMIA, comment l'organisme évalue-t-il et gère-t-il les biais potentiels des algorithmes ou modèles d'IA susceptibles d'être utilisés ?

PECB

45

### Exemples de questions fermées :

- 1 L'organisme a-t-il mis en œuvre des mesures ou des politiques spécifiques liées au management de l'IA ?
- 2 Les processus de l'organisme sont-ils contrôlés ?
- 3 Toutes les parties intéressées ont-elles été informées des processus existants ?
- 4 Existe-t-il une session de formation dans l'organisme ?
- 5 L'organisme documente-t-il ses processus ?

### Autres questions ouvertes:

- Comment l'organisme gère-t-il actuellement la gouvernance et la supervision des initiatives en matière d'IA en l'absence de SMIA?
- Pouvez-vous décrire les processus existants pour l'identification, l'évaluation et l'adoption des technologies d'IA au sein de l'organisme?
- Quels mécanismes l'organisme a-t-il mis en place pour garantir la transparence et la redevabilité dans la prise de décision en matière d'IA en l'absence d'un système de management structuré?

### Autres questions fermées:

- Les processus liés à l'IA au sein de l'organisme font-ils l'objet d'une surveillance et de contrôles réguliers?
- Des mesures ont-elles été mises en œuvre au sein de l'organisme pour répondre spécifiquement aux considérations éthiques liées à l'utilisation de l'IA?

La détermination de l'état actuel du SMIA peut être effectuée par l'équipe de projet ou confiée à des consultants externes. Les consultants externes peuvent générer des rapports plus neutres à l'égard de l'organisme que l'équipe de projet. Dans la plupart des cas, l'état actuel d'un système de management est déterminé par les rapports reçus à partir de questionnaires qui, selon le choix ou le contexte, seront envoyés par écrit ou par voie électronique.

Lors de l'utilisation de questionnaires, les questions posées pourront être:

- **Ouvertes:** Ce type de questions génère des réponses détaillées et claires. Les enquêteurs obtiennent ainsi des informations plus précieuses et plus complètes sur le système de management. Cependant, ces réponses peuvent parfois être difficiles à analyser en raison de la longueur du contenu ou du taux de réponse.
- **Fermées:** Ce type de questions génère des réponses plus facilement et plus rapidement. Ce type de questions est utile pour obtenir des opinions générales sur le système de management. Mais les enquêteurs ne disposent pas des informations ou du raisonnement qui sous-tendent les réponses.

## 1.5.2 Établir des objectifs de maturité

### Analyse des écarts et niveaux de maturité

Les objectifs des processus et des mesures d'IA peuvent être fixés en fonction des niveaux cibles de maturité :



PECB

46

**0. Inexistant** : L'organisme n'est pas conscient de l'absence totale de processus identifiables.

**1. Initial**: L'organisme a mis en œuvre certains processus, mais sans procédure normalisée.

**2. Géré**: L'organisme a mis en œuvre certains processus à l'aide de procédures uniformes, mais il n'y a pas de sessions de formation et de communication concernant ces procédures. Les personnes chargées de la mise en œuvre de ces processus s'appuient sur leurs connaissances personnelles, ce qui augmente la probabilité d'erreur.

**3. Défini**: L'organisme a normalisé, documenté et communiqué les procédures lors des sessions de formation. Toutefois, une marge d'erreur subsiste puisque ces procédures ne sont utilisées que dans le cadre d'initiatives individuelles.

**4. Géré quantitativement**: L'organisme est en mesure de contrôler et de mesurer si ces processus sont mis en œuvre comme il se doit et de prendre des mesures lorsque les procédures ne sont pas pleinement fonctionnelles. L'organisme améliore constamment ces processus, mais le recours à l'automatisation et aux outils est limité ou partiel.

**5. Optimisé**: Les processus de l'organisme ont atteint un niveau de qualité supérieure grâce à une amélioration continue et au respect des meilleures pratiques. Les ordinateurs sont utilisés pour automatiser le flux de travail intégré afin d'améliorer la qualité et l'efficacité et de permettre à l'organisme de s'adapter rapidement à de nouvelles situations.

# Analyse des écarts dans le contexte d'ISO/IEC 42001

## Exemple 1

Article	Exigence	Description de la situation actuelle	Maturité actuelle	Maturité ciblée	Analyse des écarts	Responsable
Annexe A.2.4 <i>Revue de la politique d'IA</i>	<i>La politique en matière d'IA doit être revue à des intervalles planifiés ou additionnellement en cas de besoin, afin de s'assurer de sa pertinence, de son adéquation et de son efficacité continues.</i>	La dernière revue de la politique d'IA remonte à deux ans. Bien qu'elle couvre les principes de base de l'éthique et de l'utilisation de l'IA, elle n'a pas été mise à jour pour refléter les progrès récents de la technologie et de la réglementation en matière d'IA. L'efficacité de la politique n'est pas régulièrement évaluée et aucun calendrier n'a été établi pour sa revue.	2	4	La politique d'IA est obsolète et ne fait pas l'objet d'un processus de revue systématique.	Emma TiWang, Analyste de politique d'IA

PECB

47

La liste des mesures d'IA de la norme ISO/IEC42001 (Annexe A) peut être utilisée pour l'identification des mesures d'IA existantes et planifiées dans un organisme. Cela permet d'avoir un aperçu de la situation actuelle en ce qui concerne les bonnes pratiques de sécurité.

Ce document résume l'analyse des écarts qui a été faite au sein d'un organisme en mettant l'accent sur les actions à entreprendre en priorité. Son objectif à court terme est de favoriser la mise en œuvre de mesures correctives ou préventives pour les actifs avec un risque potentiel élevé. À long terme, ce modèle de rapport permet de suivre les mesures prévues et l'analyse des écarts effectuée, en mettant l'accent sur l'amélioration continue du SMIA.

# Analyse des écarts dans le contexte d'ISO/IEC 42001

## Exemple 2

Article	Exigence	Description de la situation actuelle	Maturité actuelle	Maturité ciblée	Analyse des écarts	Responsable
<b>Annexe A.3.3 Signalement des préoccupations</b>	<i>L'organisme doit définir et mettre en place un processus de signalement des préoccupations concernant le rôle de l'organisme à l'égard d'un système d'IA tout au long de son cycle de vie.</i>	L'organisme ne dispose pas actuellement d'un processus formalisé pour signaler les préoccupations en matière d'IA. Il existe des canaux informels, mais ils ne sont pas spécifiquement adaptés aux systèmes d'IA et ne sont pas largement communiqués ou compris par les employés.	1	3	Il n'existe pas de mécanisme établi pour signaler les préoccupations en matière d'IA, ce qui peut entraîner des risques éthiques et opérationnels non traités.	Emily Lee, Responsable de communication IA

PECB

48

## 1.5.3 Présenter un rapport d'analyse des écarts

### Exemple de contenu d'un rapport d'analyse des écarts

- Introduction
  - ▷ Objectif du rapport
  - ▷ Méthodologie
- Base de référence des processus et mesures actuels de l'IA
  - ▷ Outils et processus disponibles
  - ▷ Défis posés par les outils, les processus et les ressources disponibles
- Cadre décisionnel axé sur l'IA
  - ▷ Identifier et sélectionner un projet
  - ▷ Prévoir les résultats du projet SMIA
  - ▷ Mettre en œuvre le projet SMIA
- Identification et analyse des écarts
- Options de transition suggérées
- Résumé et étapes suivantes

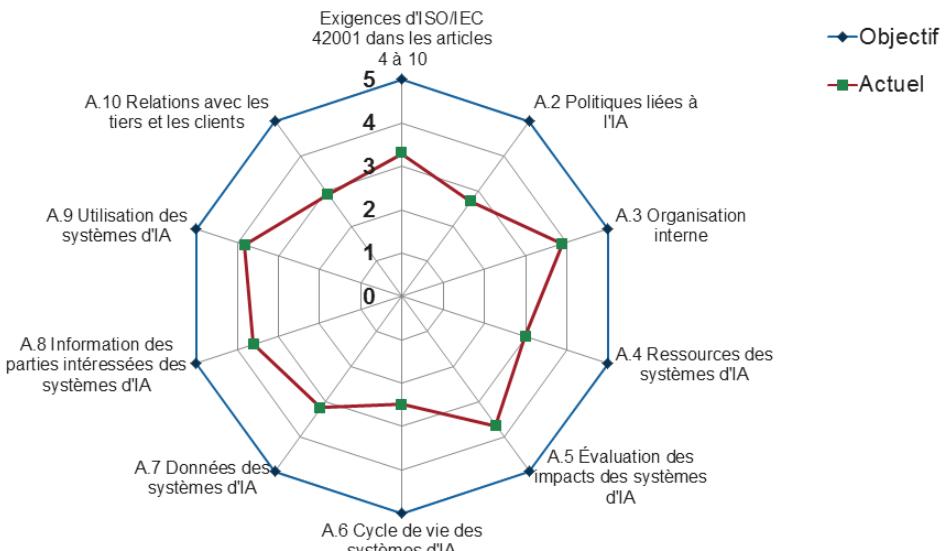


PECB

49

# Rapport d'analyse des écarts

## Exemple de représentation graphique



PECB

50

Il est important d'illustrer les différences constatées par une représentation graphique. Il est ainsi plus facile d'identifier les éléments positifs et ceux qui doivent encore être améliorés.

Dans le graphique «en radar» (aussi appelé «en toile d'araignée») ci-dessus, il y a autant d'axes qu'il y a de catégories.

Les catégories représentant les éléments du système de management de l'intelligence artificielle (ISO/IEC42001) partent toutes du point central selon une séquence horaire classique. Elles sont indiquées autour du graphique (axe des X). Les valeurs de la série (ici, les valeurs attribuées par l'analyse de la maturité du processus) sont affichées à l'intérieur de la toile (axe des Y) sur une échelle impaire allant de 1 à 5.

La présentation en cercles concentriques ici utilisée peut varier selon que les segments de droite (lignes) relient les données d'une série, formant une «toile d'araignée» dont la forme variera à son tour en fonction du nombre de séries et des valeurs attribuées à chaque catégorie du graphique.

Les avantages de cette représentation comprennent:

- On peut présenter plusieurs séries de données dans un seul graphique.
- Elle est utilisée dans divers domaines pour mettre en valeur une série par rapport à une autre, les «toiles d'araignée» superposées donnant une bonne vue d'ensemble d'une situation.

# Résumé de la section :

- Une analyse des écarts est menée dans le but de déterminer les étapes à suivre pour passer d'un état actuel à un état futur souhaité.
- Les procédures de collecte d'informations les plus couramment utilisées sont : les observations, les questionnaires, les entretiens, les revues des informations documentées et les outils de diagnostic.
- Il existe six niveaux de maturité utiles pour fixer des objectifs pour les processus et les mesures d'IA : inexistant, initial, géré, défini, géré quantitativement et optimisé.
- Un rapport d'analyse des écarts comprend généralement une introduction, un état des lieux des processus ou mesures actuels d'IA, un cadre décisionnel axé sur l'IA, l'identification et l'analyse des écarts, des options de transition suggérées, un résumé et les étapes à venir.



Questions ?



Quiz 9

PECB

51

**Note:**Pour répondre au Quizz9, veuillez accéder à la fiche Quizz.

# Section 11

## Politique d'IA

- Types de politiques
- Modèles de politiques
- Politique d'IA
- Politiques d'IA spécifiques
- Approbation des politiques par la direction
- Publication et diffusion des politiques
- Contrôle, évaluation et revue des politiques

PECB

52

Cette section fournit des informations qui aideront les participants à obtenir un aperçu des types et des modèles de politiques. Elle explique également comment rédiger, communiquer et revoir les politiques d'IA et les politiques de sécurité spécifiques.

# Politique d'IA

1. Définir et établir		2. Mettre en œuvre et opérer		3. Surveiller et revoir		4. Maintenir et améliorer	
1.1	Leadership et approbation du projet	2.1	Sélection et conception des mesures	3.1	Surveillance, mesurage, analyse et évaluation	4.1	Traitement des non-conformités
1.2	Rôles et responsabilités	2.2	Mise en œuvre des mesures	3.2	Audit interne	4.2	Amélioration continue
1.3	L'organisme et son contexte	2.3	Gestion des informations documentées	3.3	Revue de direction		
1.4	Périmètre du SMIA	2.4	Communication				
1.5	Analyse du système existant	2.5	Compétence et sensibilisation				
1.6	<b>Politique d'IA</b>	2.6	Gestion des opérations d'IA				
1.7	Management du risque lié à l'IA						
1.8	Déclaration d'applicabilité						

PECB

53

# Exigences d'ISO/IEC 42001 en termes de politique d'IA

ISO/IEC 42001, articles 5.2 et 5.1

## 5.2. Politique

La direction doit établir une politique de l'IA qui:

- a) est adaptée à la mission de l'organisme;
- b) fournit un cadre pour la définition des objectifs d'IA;
- c) inclut l'engagement de répondre aux exigences applicables;
- d) inclut l'engagement d'œuvrer pour l'amélioration continue du système de management de l'IA.

La politique d'IA doit:

- être disponible sous forme d'information documentée;
- être communiquée au sein de l'organisme;
- être mise à la disposition des parties intéressées, le cas échéant.

## 5.1. Leadership et engagement

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management de l'IA, en:

- s'assurant qu'une politique et des objectifs sont établis en matière d'IA et qu'ils sont compatibles avec l'orientation stratégique de l'organisme;

PECB

54

Pour se conformer aux exigences de la norme ISO/IEC42001, il convient à l'organisme de:

1. Publier la politique d'IA
2. Communiquer les politiques aux parties intéressées concernées

**ISO/IEC42001, B.2.2 Politique d'IA**

**Recommandations de mise en œuvre**

Il convient que la politique d'IA s'appuie sur:

- la stratégie commerciale;
- les valeurs et la culture organisationnelles et le niveau de risque que l'organisme est prêt à assumer ou à conserver;
- le niveau de risque posé par les systèmes d'IA;
- les exigences légales, y compris les contrats;
- l'environnement de risque de l'organisme;
- l'impact sur les parties intéressées concernées.

Il convient que la politique d'IA contienne:

- les principes guidant toutes les activités de l'organisme en relation avec l'IA;
- les processus de traitement des écarts et des exceptions à la politique.

Il convient que la politique d'IA prenne en considération des aspects spécifiques à une thématique lorsque cela s'avère nécessaire pour fournir des lignes directrices supplémentaires ou des références croisées avec d'autres politiques traitant de ces aspects. Ces thématiques peuvent inclure:

- les ressources et actifs de l'IA;
- les évaluations d'impact des systèmes d'IA;
- le développement de systèmes d'IA.

Il convient que des politiques pertinentes guident le développement, l'achat, l'exploitation et l'utilisation des systèmes d'IA.

# La différence entre politique et ligne directrice

---

## Politique

---

L'article 3.5 de la norme ISO/IEC 42001 définit une politique comme étant les « intentions et orientation d'un organisme telles que formalisées par sa direction. »

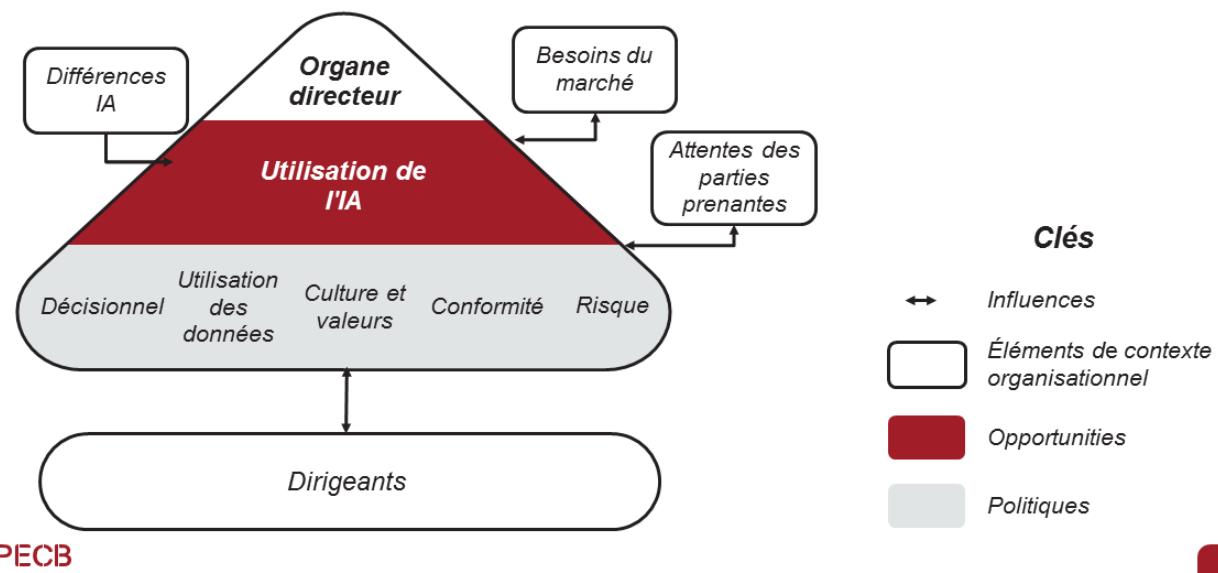
## Ligne directrice

---

Une ligne directrice est un document énonçant une règle générale, un principe ou une information sur la manière de mener une activité.

# Politiques et structure de gouvernance de l'IA

ISO/IEC 38507, Figure 3



56

Le diagramme indique que les politiques constituent l'élément fondamental de la structure de gouvernance de l'IA au sein d'un organisme. La position des politiques dans le diagramme, par rapport à la section des dirigeants du bas, suggère que les politiques sont un résultat ou un outil clé pour les dirigeants afin de mettre en œuvre la gouvernance de l'IA établie par l'organe directeur.

## ISO/IEC38507, article6.1 Généralités

*Le maintien d'une gouvernance efficace exige de revoir et éventuellement de renforcer les mécanismes et contrôles de gouvernance existants pour s'assurer qu'ils sont robustes, explicites et appropriés pour couvrir les considérations de gouvernance supplémentaires (ainsi que d'orientation pour la direction) que les systèmes d'IA apportent à l'organisme et à ses parties prenantes.*

*Il convient en outre que l'organe de direction et les dirigeants impliquent les parties prenantes susceptibles d'être affectées par l'utilisation des systèmes d'IA, telles que le personnel et ses représentants, tout au long du processus de mise en œuvre des systèmes d'IA dans les organismes, par le biais de procédures d'information, de consultation et de participation.*

*Les orientations contenues dans le présent article visent à aider l'organe directeur à comprendre et à réviser les politiques qu'il convient de prévoir afin de réduire les conséquences évitables et involontaires de l'utilisation de l'IA par l'organisme. Elles ne sont pas et ne peuvent pas être exhaustives.*

*Selon la norme ISO/IEC TR 38502:2017, 4.1.3, les dirigeants sont chargés d'assurer la réalisation des objectifs de l'organisme dans le cadre des stratégies et des politiques établies par l'organe directeur. La tâche de gouvernance est accomplie en étroite collaboration entre l'organe directeur et les dirigeants, comme illustré par la figure3.*

# 1.6 Politique d'IA

## Liste des activités

1.6.1

Créer des modèles de politiques

1.6.4

Obtenir l'approbation des politiques par la direction

1.6.2

Rédiger la politique d'IA

1.6.5

Publier et diffuser les politiques

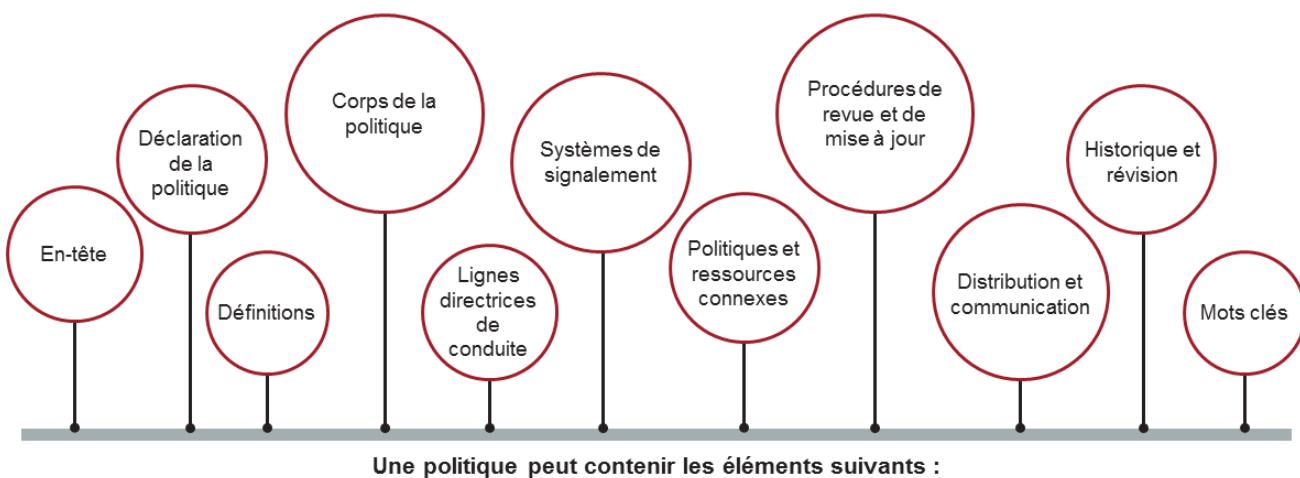
1.6.3

Rédiger des politiques d'IA spécifiques

1.6.6

Contrôler, évaluer et revoir les politiques

## 1.6.1 Créer des modèles de politiques



PECB

58

### En-tête

- **Titre** : Définir de manière claire et concise l'objet de la politique
- **Signature d'approbation** : Signatures des approbateurs, indiquant l'autorisation et l'approbation
- **Département** : Préciser le département responsable de la politique

### Déclaration de la politique

- **Objectif** : Articuler l'objectif de la politique et la manière dont elle profite à l'organisme
- **Périmètre** : Définir qui et quoi est concerné par la politique
- **Date d'entrée en vigueur** : Préciser la date d'entrée en vigueur de la politique

### Définitions

- **Termes clés** : Expliquer les termes techniques ou spécialisés utilisés dans la politique pour plus de clarté

### Corps de la politique

- **Contexte et argumentaire** : Fournir le contexte et les raisons de la politique, en la reliant aux objectifs de l'entreprise
- **Détails de la politique** : Décrire les règles, les lignes directrices et les normes spécifiques
- **Processus et procédures** : Décrire, étape par étape, les actions ou les procédures nécessaires à la mise en conformité
- **Rôles et responsabilités** : Définir clairement qui est responsable de quelles actions et décisions
- **Alternatives et flexibilité** : Le cas échéant, mentionner des options alternatives ou des domaines de flexibilité dans la politique

### Lignes directrices de conduite

- **Comportements attendus** : Détailler les comportements ou les actions attendus dans le cadre de la politique
- **Conséquences** : Énoncer clairement les répercussions des violations de la politique, y compris les mesures disciplinaires

# Page de notes

---

PECB

59

## Systèmes de signalement

- **Mécanismes de signalement** : Fournir des instructions sur la manière de signaler les violations ou les préoccupations
- **Informations de contact** : Liste des coordonnées pertinentes (par exemple, adresses électroniques, numéros de téléphone)

## Politiques et ressources connexes

- **Documents de référence** : Lien vers les politiques, procédures, formulaires, lignes directrices et autres ressources connexes
- **Conformité légale** : Mentionner toute loi ou réglementation pertinente à laquelle la politique adhère

## Procédures de revue et de mise à jour

- **Calendrier de revue** : Indiquer à quelle fréquence et par qui la politique sera revue
- **Processus de mise à jour** : Décrire la procédure à suivre pour apporter des modifications à la politique

## Distribution et communication

- **Plan de distribution** : Décrire comment la politique sera communiquée et distribuée aux employés
- **Exigence de reconnaissance** : Si nécessaire, inclure une section permettant aux employés de reconnaître qu'ils ont lu et compris la politique

## Historique et révision

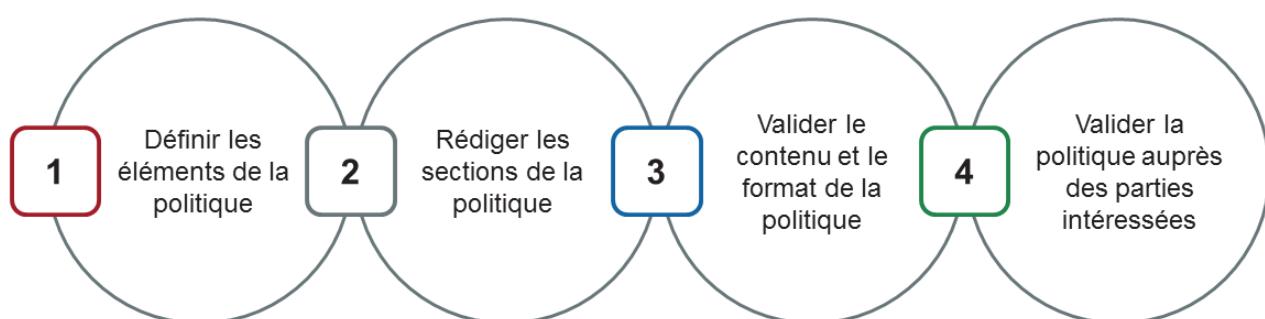
- **Journal des changements** : Documenter l'historique des changements importants, y compris les dates et les descriptions des révisions

## Mots clés

- **Termes de recherche** : Inclure des mots-clés relatifs à la politique pour faciliter la recherche et le référencement.

## 1.6.2 Rédiger la politique d'IA

### Processus de rédaction d'une politique



PECB

60

Les étapes classiques du processus de rédaction d'une politique sont les suivantes:

1. **Définir les éléments de la politique :** L'équipe chargée de la politique dresse une liste de tous les sujets qui doivent être traités dans la politique. La politique doit au moins couvrir les exigences de l'article 5.2 de la norme ISO/IEC42001 *Politique*.
2. **Rédiger les sections de la politique:** La personne responsable de la rédaction de la politique rédige les différentes sections de la politique. Il faut s'assurer que les énoncés emploient un langage simple, mais précis afin que la politique soit comprise par toutes les parties concernées par sa publication. En outre, il faut éviter d'inclure des spécifications opérationnelles ou des références à des produits particuliers dans la politique. La politique devrait aborder le «Pourquoi» et surtout le «Quoi», et non le «Comment». Le «Comment» sera détaillé dans les procédures.
3. **Valider le contenu et le format de la politique:** La personne chargée de rédiger la politique doit en valider le contenu afin de s'assurer que la politique est conforme aux exigences de la norme ISO/IEC 42001 et aux autres politiques de l'organisme. Par exemple, il serait contradictoire de publier une politique autorisant la surveillance de toutes les communications des employés si une politique de l'organisme sur le respect de la vie privée l'interdit. En termes de format, la personne doit s'assurer que la politique répond aux exigences de l'article 7.5.3 *Contrôle des informations documentées* de la norme ISO/IEC42001.
4. **Valider la politique auprès des parties intéressées:** Pour s'assurer que la politique est comprise par toutes les parties concernées, il convient que l'organisme obtienne un retour d'information de leur part. Cette étape peut durer un certain temps, en fonction du nombre de parties intéressées.

Il convient qu'une personne soit désignée comme responsable de l'élaboration, de la revue et de l'évaluation de la politique.

# Exemple d'une politique d'IA

Résumé	Cette politique vise à assurer un développement et un déploiement responsables et éthiques des systèmes d'IA par l'organisme, dans le respect des normes juridiques et éthiques, en mettant l'accent sur la transparence, la redevabilité et l'équité.
Introduction	L'organisme s'engage à développer et à utiliser des systèmes d'IA d'une manière qui respecte les droits humains, favorise l'inclusion et évite les préjudices tout en apportant des bénéfices.
Périmètre	Cette politique s'applique à tous les départements, processus ou activités de l'organisme inclus dans le périmètre du SMIA.
Objectifs	L'organisme vise à assurer la continuité d'activité opérationnelle essentielle, à veiller à ce que les systèmes d'IA soient utilisés pour améliorer la prise de décision humaine, à identifier et à apprécier régulièrement les risques liés à l'IA afin de mettre en œuvre les mesures appropriées, et à assurer la supervision des systèmes d'IA tout au long de leur cycle de vie.
Principes	Équité et non-discrimination dans les sorties de l'IA Transparence et explicabilité des processus décisionnels en matière d'IA Protection de la vie privée et gouvernance des données pour les jeux de données utilisés par l'IA Sécurité des systèmes d'IA contre les abus et les attaques malveillantes Redevabilité des décisions des systèmes d'IA et de leurs impacts Surveillance et évaluation continues des systèmes d'IA pour assurer la conformité en matière d'éthique Engagement avec les parties prenantes pour comprendre les impacts sociétaux de l'IA

PECB

61

# Exemple d'une politique d'IA (suite)

<b>Responsabilités</b>	La direction est chargée de s'assurer que les objectifs et les plans du SMIA sont établis et revus annuellement lors des réunions de revue de direction, que les rôles et les responsabilités en matière d'IA sont définis, que des programmes de sensibilisation sont menés, qu'un audit interne est réalisé au moins une fois par an et que les ressources nécessaires pour maintenir et améliorer le SMIA sont fournies. Le délégué à l'éthique de l'IA (DEIA) est chargé d'intervenir sur tous les aspects de l'IA d'un organisme. Il décide, en général, de toutes les exigences pour le fonctionnement efficace du SMIA au moyen de directives administratives, préalablement soumises à la direction générale. Chaque cadre doit veiller à ce que les systèmes d'IA développés ou utilisés par son équipe soient conformes aux politiques de l'organisme. Tous les utilisateurs (direction, employés, sous-traitants et utilisateurs tiers) devraient connaître les risques liés à l'IA, leurs responsabilités et la nécessité de respecter les politiques pour assurer un déploiement et une utilisation responsables de l'IA.
<b>Principaux résultats</b>	Développement et utilisation éthiques de l'IA Transparence et redevabilité dans les décisions relatives à l'IA Réduction des biais et de la discrimination par les systèmes d'IA Réponse et résolution rapides des incidents liés à l'IA
<b>Politiques connexes</b>	Politique d'éthique de l'IA, politique de gouvernance des données, politique de protection de la vie privée, politique de transparence de l'IA, politique de déploiement responsable de l'IA, etc.
<b>Exigences</b>	Les systèmes d'IA doivent être conçus et testés dans un souci d'équité, de redevabilité et de transparence. Les procédures de réponse aux incidents liés à l'IA doivent être suivies pour signaler et résoudre les problèmes liés à l'éthique ou aux performances de l'IA. Des évaluations et des audits réguliers des systèmes d'IA doivent être effectués pour s'assurer qu'ils fonctionnent comme prévu et sans causer de dommages.

PECB

62

## 1.6.3 Rédiger des politiques d'IA spécifiques

### Exemple de politique sur l'utilisation éthique de l'IA

Résumé	Les systèmes et outils d'IA mis à la disposition des employés ne devraient être utilisés qu'à des fins professionnelles, en veillant à leur utilisation éthique et responsable.
Introduction	Afin d'éviter toute utilisation abusive des technologies et des données d'IA de l'organisme, tous les employés sont tenus d'utiliser les systèmes et les outils d'IA uniquement pour les applications professionnelles prévues.
Périmètre	Cette politique s'applique à tous les salariés, aux membres de la direction et au personnel contractuel qui utilisent un système ou un outil d'IA fourni par l'organisme.
Objectifs	Garantir l'utilisation éthique de l'IA, empêcher l'utilisation abusive des systèmes d'IA, éviter les sorties biaisées, promouvoir la transparence des décisions en matière d'IA et protéger les données utilisées par les systèmes d'IA contre tout accès non autorisé.
Sanctions	Tout utilisateur qui enfreint cette politique peut faire l'objet de mesures disciplinaires, pouvant aller d'une obligation de reformation à une suspension ou une résiliation définitive de contrat.
Responsabilités	La ou les personnes chargées de la gestion du SMIA ou la ou les personnes chargées de la mise en œuvre des mesures liées à l'IA sont responsables de veiller à ce que les employés respectent la présente politique.
Politiques connexes	Politique de gouvernance des données d'IA, politique de confidentialité, politique de transparence en matière d'IA.

PECB

63

## 1.6.4 Obtenir l'approbation des politiques par la direction

- Bien que les experts du domaine puissent rédiger la politique d'IA, c'est la direction qui est redevable en dernier ressort de sa mise en place. À ce titre, la direction doit donc approuver la politique d'IA avant sa publication.
- L'approbation prend généralement la forme d'une signature par la personne au sommet de la hiérarchie. Toutefois, le processus d'approbation peut être confié à un comité :
  - ▷ Conseil d'administration
  - ▷ Comité de gestion
  - ▷ Comité de gouvernance de la sécurité



PECB

64

### **ISO/IEC42001, A.2.2 Politique d'IA**

*L'organisme doit documenter une politique de développement ou d'utilisation des systèmes d'IA.*

### **ISO/IEC42001, A.2.3 Alignement sur les autres politiques de l'organisme**

*L'organisme doit déterminer dans quelle mesure d'autres politiques peuvent être affectées par les objectifs de l'organisme en matière de systèmes d'IA ou s'y appliquer.*

## 1.6.5 Publier et diffuser les politiques

### Principaux modes de communication



Intranet



Réunion



Distribution de copies papier



Intégration de l'employé

PECB

65

Lors de la publication initiale de la politique d'IA de l'organisme, la bonne pratique, bien que facultative, consiste à faire signer la politique par tous les salariés de l'organisme, y compris l'équipe de direction. L'original du formulaire signé devrait être conservé par le département des ressources humaines. La présentation de preuves démontrant que les parties intéressées ont été informées peut s'avérer utile lors d'un audit de certification.

Si la signature de la politique n'est pas effectuée, l'organisme devrait s'assurer de pouvoir démontrer que des membres de l'organisme comprennent et respectent la politique. Cela peut se faire, par exemple, en participant à une session de formation.

## 1.6.6 Surveiller, évaluer et revoir la politique

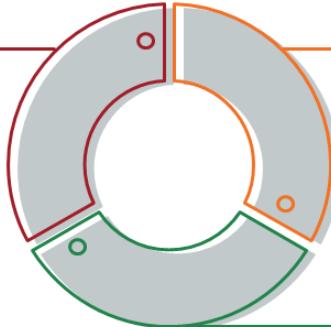
Revoir, surveiller et évaluer la politique d'IA facilite l'amélioration continue.

### Revue

Revoir régulièrement la politique pour s'assurer de sa pertinence et de son adéquation

### Surveillance

Veiller à ce que la politique soit respectée dans les opérations quotidiennes



### Évaluation

Évaluer l'efficacité et l'application de la politique

PECB

66

En révisant régulièrement la politique d'IA, l'organisme s'assure de sa cohérence avec les besoins commerciaux et les contraintes légales.

**Mesure:** La direction doit s'assurer que la politique d'IA est respectée dans les opérations quotidiennes de l'organisme. Elle doit également prévoir un processus disciplinaire formel pour les salariés qui enfreignent la politique. Au cours de ce processus, des facteurs tels que la nature et la gravité de la violation et son impact commercial devraient être pris en compte.

**Évaluation :** L'organisme doit mettre en place des mécanismes pour évaluer l'efficacité et l'application de sa politique d'IA.

**Revue:** Pour assurer sa pertinence, son adéquation et son efficacité, il convient de réexaminer la politique à intervalles planifiés ou en cas de changements majeurs. Les organismes revoient souvent la politique d'IA lors des revues de direction.

## Résumé de la section :

- Le processus de rédaction d'une politique comprend les étapes suivantes : définition des composantes de la politique, rédaction des sections de la politique, validation du contenu et du format de la politique et validation de la politique avec les parties intéressées.
- La politique d'IA et les politiques spécifiques devraient être communiquées au personnel concerné et aux parties intéressées sous une forme pertinente, accessible et compréhensible par leurs destinataires.
- Revoir, surveiller et évaluer la politique d'IA facilite l'amélioration continue.



Questions ?



Quiz 10

PECB

67

**Note:**Pour répondre au Quizz10, veuillez accéder à la fiche Quizz.

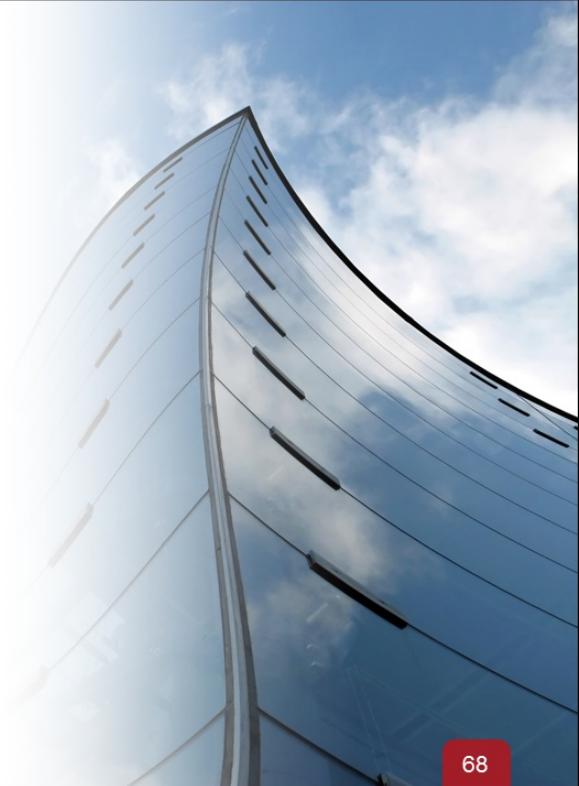
# Section 12

## Management du risque lié à l'IA

- ISO 31000
- Principes du management du risque lié à l'IA
- Périmètre, contexte et critères
- Identification du risque
- Analyse du risque
- Évaluation du risque
- Traitement du risque
- Communication et consultation
- Enregistrement et élaboration de rapports
- Surveillance et revue

PECB

68



Cette section fournit des informations qui aideront les participants à comprendre les principes de management des risques liés à l'IA et les principaux processus de management de risques IA, notamment le périmètre, le contexte et les critères, l'appréciation du risque, le traitement du risque, la communication et la consultation, l'enregistrement et l'élaboration de rapports, ainsi que la surveillance et la revue.

# Management du risque lié à l'IA

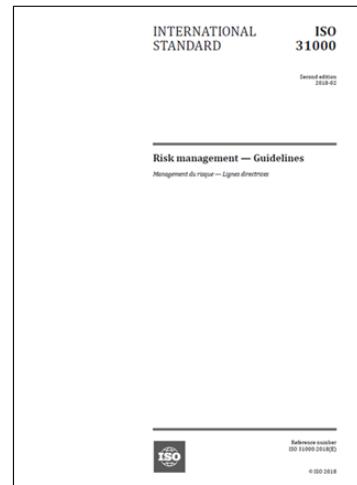
1. Définir et établir		2. Mettre en œuvre et opérer		3. Surveiller et revoir		4. Maintenir et améliorer	
1.1	Leadership et approbation du projet	2.1	Sélection et conception des mesures	3.1	Surveillance, mesurage, analyse et évaluation	4.1	Traitement des non-conformités
1.2	Rôles et responsabilités	2.2	Mise en œuvre des mesures	3.2	Audit interne	4.2	Amélioration continue
1.3	L'organisme et son contexte	2.3	Gestion des informations documentées	3.3	Revue de direction		
1.4	Périmètre du SMIA	2.4	Communication				
1.5	Analyse du système existant	2.5	Compétence et sensibilisation				
1.6	Politique d'IA	2.6	Gestion des opérations d'IA				
1.7	<b>Management du risque lié à l'IA</b>						
1.8	Déclaration d'applicabilité						

PECB

69

# ISO 31000 : Management du risque — Lignes directrices

- La norme ISO 31000 fournit des lignes directrices, des principes et un cadre pour le management des risques.
- Elle peut s'appliquer à tout type de risque, indépendamment de sa nature ou de ses conséquences.
- Elle n'est pas destinée à des fins de certification.



PECB

70

## ISO 31000, article 1 Domaine d'application

Le présent document fournit des lignes directrices concernant le management du risque auquel sont confrontés les organismes. L'application de ces lignes directrices peut être adaptée à tout organisme et à son contexte.

Le présent document fournit une approche générique permettant de gérer toute forme de risque et n'est pas spécifique à une industrie ou un secteur.

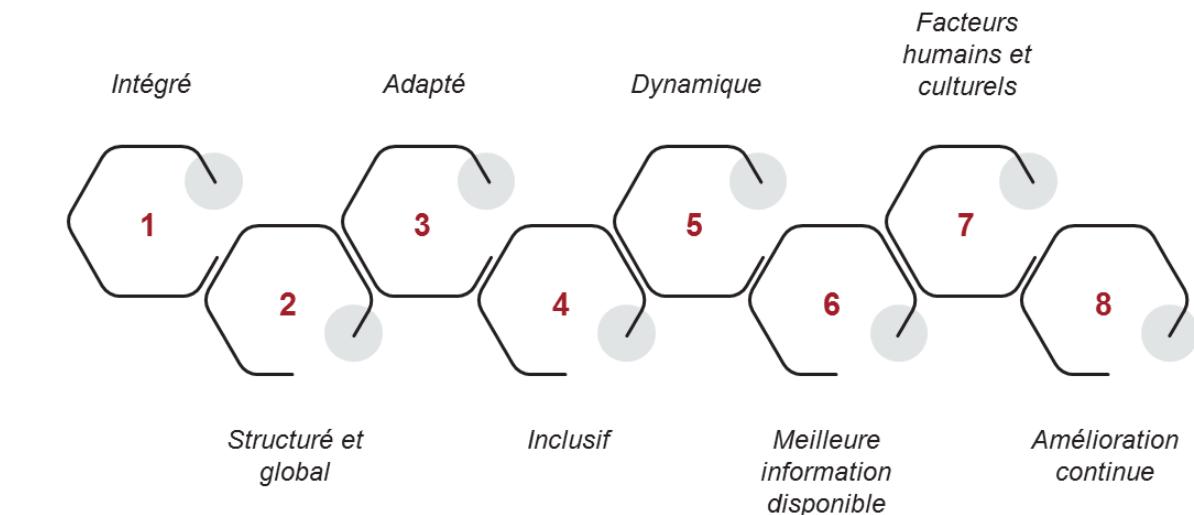
Le présent document peut être utilisé tout au long de la vie de l'organisme et peut être appliqué à toute activité, y compris la prise de décisions à tous les niveaux.

Étant donné que la norme ISO/IEC42001 ne fournit pas de méthode spécifique pour le management des risques dans le contexte du SMIA, il appartient à chaque organisme d'identifier et de sélectionner celle qui correspond à son contexte, à ses activités commerciales et à ses pratiques opérationnelles et de management.

Dans cette section, le processus de management des risques est expliqué en faisant référence à des normes spécifiques à des fins informatives; il est essentiel de noter que l'adhésion à ces normes n'est pas obligatoire pour se conformer à la norme ISO/IEC42001.

# Principes du management du risque lié à l'IA

ISO/IEC 23894, Tableau 1



PECB

71

## ISO/IEC23894, article4 Principes du management du risque lié à l'IA

*Il convient que le management du risque aborde les besoins de l'organisme à l'aide d'une approche intégrée, structurée et globale. Des principes directeurs permettent à un organisme d'identifier des priorités et de prendre des décisions sur la façon de gérer les effets de l'incertitude sur ses objectifs. Ces principes s'appliquent à tous les niveaux et objectifs organisationnels, qu'ils soient stratégiques ou opérationnels.*

*Les systèmes et processus déploient habituellement une combinaison de plusieurs technologies et fonctionnalités dans divers environnements, pour des cas d'utilisation spécifiques. Il convient que le management du risque tienne compte du système dans sa globalité, avec toutes ses technologies, ses fonctionnalités, son impact sur l'environnement et ses parties prenantes.*

*Les systèmes d'IA peuvent introduire des risques nouveaux ou émergents pour un organisme, avec des conséquences positives ou négatives sur ses objectifs, ou une modification de la vraisemblance des risques existants. Ils peuvent également nécessiter une considération spécifique de la part de l'organisme. Des recommandations additionnelles pour les principes de management du risque, le cadre organisationnel et les processus qu'un organisme peut mettre en œuvre sont fournies dans le présent document.*

**NOTE** La définition du mot «risque» peut différer significativement dans les différentes Normes internationales. Dans l'ISO31000:2018 et les normes associées, «risque» implique un écart positif ou négatif par rapport à des objectifs. Dans d'autres Normes internationales, «risque» implique des conséquences potentiellement négatives uniquement, par exemple, des préoccupations relatives à la sûreté. Cette différence de perspective peut fréquemment porter à confusion lorsqu'il s'agit d'essayer de comprendre et de mettre en œuvre correctement un processus de management du risque conforme.

*L'Article4 de l'ISO31000:2018 définit plusieurs principes génériques pour le management du risque. Outre les recommandations données dans l'ISO31000:2018, Article4, le Tableau1 fournit des recommandations supplémentaires relatives à la façon d'appliquer ces principes, le cas échéant.*

# Intégré

## ISO/IEC 23894, Tableau 1

### Description

*Le management du risque est intégré à toutes les activités de l'organisme.*

### Fondement

Les deux principales méthodes d'application de ce principe sont les suivantes :

- L'élaboration du cadre de management des risques (y compris l'évaluation et l'amélioration)
- L'application du processus de management des risques au niveau de la prise de décision et des activités connexes

# Structuré et global

ISO/IEC 23894, Tableau 1

## Interprétation

*Une approche structurée et globale du management du risque contribue à la cohérence de résultats qui peuvent être comparés.*

## Application

Une approche cohérente du management des risques rendra l'organisme plus efficace et lui permettra d'atteindre les résultats escomptés. Cela nécessite des pratiques organisationnelles qui prennent en compte les risques associés au contexte organisationnel, l'utilisation de critères de risque cohérents et conformes aux objectifs de l'organisme, ainsi que le périmètre des activités de l'organisme.

PECB

73

# Adapté

## ISO/IEC 23894, Tableau 1

### Interprétation

*Le cadre organisationnel et le processus de management du risque sont adaptés et proportionnés au contexte externe et interne de l'organisme aussi bien qu'à ses objectifs.*

### Application

Le cadre et le processus de management des risques devraient être adaptés aux besoins de l'organisme. Il n'existe pas de méthode universelle pour les concevoir, car ils requièrent souplesse et adaptation, en fonction du contexte spécifique de l'organisme. La conception peut être déterminée par de nombreux aspects, notamment la taille de l'organisme, sa culture, son secteur et son style de management.

PECB

74

# Inclusif

## ISO/IEC 23894, Tableau 1

### Interprétation

*L'implication appropriée et au moment opportun des parties prenantes permet de prendre en compte leurs connaissances, leurs opinions et leur perception. Cela conduit à un management du risque mieux éclairé et plus pertinent.*

### Application

Les organisations devraient impliquer divers groupes internes et externes dans une discussion sur les incidences potentielles de l'IA. Les parties prenantes jouent un rôle crucial dans l'identification des risques liés aux données dans l'apprentissage machine, dans la résolution des problèmes de transparence et dans la définition des critères d'équité pour la prise de décision automatisée. Leur contribution est essentielle pour intégrer le retour d'information et la sensibilisation dans le processus de management des risques, compte tenu des parties prenantes supplémentaires introduites par l'IA.

# Dynamique

## ISO/IEC 23894, Tableau 1

### Interprétation

*Des risques peuvent surgir, être modifiés ou disparaître lorsque le contexte externe et interne d'un organisme change. Le management du risque anticipe, détecte, reconnaît et réagit à ces changements et événements en temps voulu et de manière appropriée.*

### Application

Pour se conformer à la norme ISO 31000:2018, les organismes doivent établir des structures pour identifier les risques émergents dans les systèmes d'IA. Un management dynamique du risque est essentiel en raison de l'apprentissage continu et de la nature adaptative de l'IA. Les attentes élevées des clients et l'évolution des exigences légales en matière d'IA exigent une adaptation constante. L'intégration des risques liés à l'IA dans les systèmes de management existants offre une approche globale pour relever ces défis évolutifs.

PECB

76

# Meilleure information disponible

## ISO/IEC 23894, Tableau 1

### Interprétation

*Les données d'entrée du management du risque sont fondées sur des informations historiques et actuelles ainsi que sur les attentes futures. Le management du risque tient compte explicitement de toutes limites et incertitudes associées à ces informations et attentes. Il convient que les informations soient disponibles à temps, claires et accessibles aux parties prenantes pertinentes.*

### Application

Les organismes qui développent des systèmes d'IA devraient surveiller leurs utilisations futures, et les utilisateurs tenir des enregistrements de l'utilisation des systèmes d'IA. En raison de la nature évolutive de l'IA, les organismes devraient tenir compte des limites des informations historiques et être attentifs à l'évolution des attentes. Il convient d'examiner l'utilisation interne des systèmes d'IA et d'intégrer dans le processus de management des risques IA les restrictions relatives au suivi de l'utilisation externe, telles que la propriété intellectuelle ou les limites contractuelles, et de les mettre à jour si nécessaire.

PECB

77

# Facteurs humains et culturels

## ISO/IEC 23894, Tableau 1

### Interprétation

*Le comportement humain et la culture influent de manière significative sur tous les aspects du management du risque à chaque niveau et à chaque étape.*

### Application

Les organismes qui développent des systèmes d'IA devraient surveiller les utilisations futures et les utilisateurs conserver des enregistrements de l'utilisation du système. En raison de la nature évolutive de l'IA, les informations historiques peuvent être limitées et les attentes peuvent changer rapidement. L'utilisation interne des systèmes d'IA devrait être prise en compte. Le suivi de l'utilisation externe peut faire l'objet de restrictions, telles que des limites contractuelles ou de propriété intellectuelle, intégrées dans le processus de management des risques et mises à jour si nécessaire.

# Amélioration continue

## ISO/IEC 23894, Tableau 1

### Interprétation

*Le management du risque est amélioré en continu par l'apprentissage et l'expérience.*

### Application

Les organismes impliqués dans la conception, le développement ou le déploiement de systèmes d'IA devraient intégrer l'identification des risques imprévus dans leurs processus d'amélioration continue. Pour améliorer les performances, ces organismes devraient surveiller régulièrement l'écosystème de l'IA, en évaluant les réussites, les lacunes et les enseignements tirés. De plus, se tenir informé des nouveaux avancements de la recherche et des nouvelles techniques en matière d'IA offre de précieuses opportunités d'amélioration.

# Système de management du risque

## Acte sur l'IA de l'UE

- L'article 9 de l'Acte sur l'IA de l'UE impose aux fournisseurs de systèmes à haut risque de mettre en place un système de management des risques complet.
- Ce système doit être un processus continu qui fonctionne tout au long du cycle de vie du système d'IA.
- Il implique d'identifier et d'évaluer la nature, l'origine et la gravité des risques que le système d'IA pourrait présenter, puis de prendre les mesures appropriées pour éliminer ou atténuer ces risques.
- L'objectif est de s'assurer que le système d'IA est sûr et qu'il respecte les droits fondamentaux et les exigences en matière de sécurité.

PECB

80

# Cadre pour le management du risque lié à l'IA

## ISO/IEC 23894, article 5.1

- La finalité du cadre organisationnel de management du risque est d'aider l'organisme à intégrer le management du risque dans les activités et les fonctions significatives. Les recommandations données dans l'ISO 31000:2018, 5.1, s'appliquent.
- Le management du risque implique de réunir des informations pertinentes pour qu'un organisme prenne des décisions et aborde le risque. Tandis que l'organe de gouvernance définit l'appétit global pour le risque et les objectifs organisationnels, il délègue le processus de prise de décision relatif à l'identification, à l'appréciation et au traitement du risque à la direction au sein de l'organisme.
- L'ISO/IEC 38507 décrit des considérations additionnelles relatives à la gouvernance pour l'organisme en ce qui concerne le développement, l'achat ou l'utilisation d'un système d'IA. De telles considérations incluent les nouvelles opportunités, les modifications potentielles relatives à l'appétit pour le risque ainsi que les nouvelles politiques de gouvernance pour garantir l'utilisation responsable de l'IA par l'organisme. Elles peuvent être utilisées conjointement avec le processus de management du risque décrit dans le présent document pour contribuer à guider l'intégration organisationnelle dynamique et itérative décrite dans l'ISO 31000:2018, 5.2.

PECB

81

## ISO/IEC38507, article6.7.2 Management du risque

Le management du risque fait partie intégrante de toutes les activités de l'organisme. Bien que les systèmes d'IA puissent apporter des avantages à l'organisme, il convient de réviser les objectifs de l'organisme liés à la bonne gouvernance de la prise de décision, à l'utilisation des données et à la culture et aux valeurs souhaitées par l'organisme pour tenir compte des impacts possibles de l'utilisation de l'IA.

L'organisme s'efforce de protéger ses principes et ses valeurs, son identité et sa réputation, ses parties prenantes, son marché et son environnement, ainsi que sa liberté d'action, dans le but de réussir sa mission.

Pour faire face aux risques posés par l'IA, il convient que l'organe directeur mette en place:

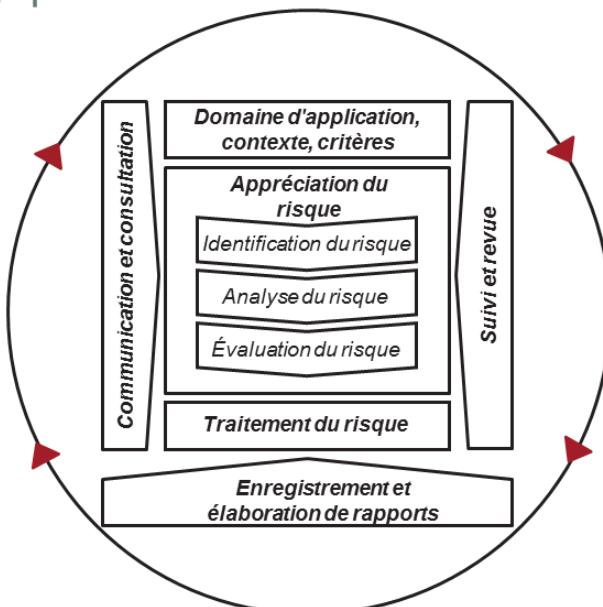
- des règles et politiques internes appropriées;
- des sous-organisations, des processus et des outils spécifiques appropriés conçus pour assurer ou appliquer les valeurs, les principes et les contrôles internes essentiels à une bonne gouvernance.

En outre, il convient que l'organe directeur veille à ce que les contractants et sous-traitants de l'organisme respectent les mêmes codes de pratique et politiques.

Ces mesures permettent à toute partie prenante d'identifier et de signaler les comportements non conformes liés au système d'IA et de recevoir des réponses significatives et adéquates. Elles sont particulièrement importantes lorsque des chaînes d'approvisionnement complexes sont impliquées et qu'un contractant principal ou un acheteur est susceptible de courir un risque de réputation, un risque financier ou un autre risque. Il convient que l'organisme acquiert une compréhension claire des implications de l'utilisation de l'IA dans le cadre de relations contractuelles où les tolérances de risque des différents organismes sont en jeu.

# Processus de management du risque selon ISO 31000

ISO 31000, Figure 4



PECB

82

Comme l'illustre la figure, le processus de management des risques devrait être itératif pour les activités d'appréciation et de traitement du risque. Si les activités d'appréciation du risque ont fourni suffisamment de preuves que les mesures déterminées réduiront les risques à un niveau acceptable, l'étape suivante consiste à mettre en œuvre des options de traitement du risque. Toutefois, si les informations sont insuffisantes pour déterminer le niveau de risque ou que le niveau de risque projeté après traitement est inacceptable, une itération de l'appréciation du risque sera menée sur certains ou tous les éléments du domaine d'application. Si l'option de traitement du risque n'est pas satisfaisante, mais que le domaine d'application, le contexte, les critères et l'appréciation du risque sont corrects, une nouvelle itération du traitement du risque sera effectuée. Dans le cas contraire, une mise à jour du champ d'application, du contexte et des critères devra également être effectuée.

L'efficacité du traitement du risque dépend en partie de l'exactitude de l'appréciation du risque. Il est possible que le traitement du risque n'aboutisse pas directement à un niveau acceptable de risque résiduel. Dans ce cas, il convient de procéder à une nouvelle itération de l'appréciation du risque.

La communication du risque aux parties intéressées de l'organisme est une activité continue, tout comme la surveillance des risques.

# Page de notes

---

PECB

83

## **ISO/IEC23894, article6.1 Généralités**

*Les recommandations données dans l'ISO31000:2018, 6.1, s'appliquent. Il convient que les organismes mettent en œuvre une approche fondée sur les risques pour identifier, apprécier et comprendre les risques liés à l'IA auxquels ils sont exposés et prendre des mesures de traitement appropriées conformément au niveau de risque. La réussite du processus global de management du risque lié à l'IA d'un organisme repose sur l'identification, l'établissement et la mise en œuvre réussie de processus de management du risque à portée ajustée aux niveaux stratégique, opérationnel, du programme et du projet. En raison de préoccupations qui se rapportent, sans s'y limiter, à la complexité, au manque de transparence et à l'imprévisibilité de certaines technologies basées sur l'IA, il convient d'apporter une considération particulière au processus de management du risque au niveau du projet des systèmes d'IA. Il convient que ces processus au niveau du projet des systèmes d'IA soient alignés avec les objectifs de l'organisme et il convient qu'ils échangent, dans les deux sens, des informations avec les autres niveaux du management du risque. Par exemple, il convient que les remontées d'informations et les enseignements tirés au niveau du projet de l'IA soient intégrés à des niveaux supérieurs, tels que les niveaux stratégique, opérationnel, du programme et autres, suivant le cas.*

*La portée, le contexte et les critères d'un processus de management du risque au niveau du projet sont directement affectés par les étapes du cycle de vie du système d'IA relevant de la portée du projet. L'Annexe C démontre des relations possibles entre un processus de management du risque au niveau du projet et le cycle de vie d'un système d'IA.*

# Appréciation du risque lié à l'IA

## ISO/IEC 42001, article 6.1.2

*L'organisme doit définir et appliquer un processus d'appréciation du risque lié à l'IA qui:*

- a) s'appuie et s'aligne sur la politique et les objectifs en matière d'IA;*

*NOTE Lors de l'évaluation des conséquences comme spécifié en 6.1.2 d) 1), l'organisme peut utiliser une évaluation d'impact de système d'IA comme indiqué en 6.1.4.*

- b) est conçu de manière à ce que la répétition des appréciations du risque d'IA produise des résultats cohérents, valides et comparables;*

- c) identifie les risques qui facilitent ou empêchent la réalisation de ses objectifs en matière d'IA;*

# Appréciation du risque lié à l'IA (suite)

## ISO/IEC 42001, article 6.1.2

d) analyse les risques liés à l'IA pour:

- 1) apprécier les conséquences potentielles pour l'organisme, les personnes et les sociétés en cas de concrétisation des risques identifiés;
- 2) apprécier, le cas échéant, la probabilité réaliste des risques identifiés;
- 3) déterminer les niveaux des risques.

e) évalue les risques liés à l'IA pour:

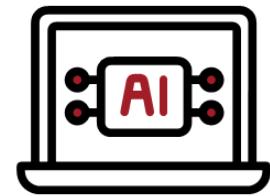
- 1) comparer les résultats de l'analyse du risque avec les critères de risque;
- 2) prioriser les risques appréciés pour le traitement du risque.

L'organisme doit conserver des informations documentées sur le processus d'appreciation du risque liés à l'IA.

# Évaluation de l'impact du système d'IA

## ISO/IEC 42001, article 6.1.4

- *L'organisme doit définir un processus d'évaluation des conséquences potentielles du développement, de la mise à disposition ou de l'utilisation de systèmes d'IA pour les personnes ou les groupes de personnes, ou les deux, et pour les sociétés.*
- *L'évaluation de l'impact des systèmes d'IA doit déterminer les conséquences potentielles du déploiement d'un système d'IA, de son utilisation prévue et de son utilisation abusive prévisible sur des personnes ou des groupes de personnes, ou les deux, et sur les sociétés.*
- *L'analyse d'impact du système d'IA doit tenir compte du contexte technique et sociétal spécifique dans lequel le système d'IA est déployé et des jurisdictions applicables.*



PECB

86

### ISO/IEC42001, article6.1.4 Évaluation de l'impact du système d'IA (suite)

*Le résultat de l'analyse d'impact du système d'IA doit être documenté. Le cas échéant, les résultats de l'analyse d'impact du système peuvent être mis à la disposition des parties intéressées concernées, telles que définies par l'organisme.*

*L'organisme doit prendre en compte les résultats de l'évaluation d'impact du système d'IA dans l'appréciation du risque. A.5 dans le tableauA.1 fournit des mesures pour l'évaluation des impacts des systèmes d'IA.*

*NOTE Dans certains contextes (tels que les systèmes d'IA critiques pour la sécurité ou la vie privée), l'organisme peut exiger que des évaluations d'impact des systèmes d'IA spécifiques à une discipline (par exemple, impact sur la sécurité, la vie privée ou la sûreté) soient réalisées dans le cadre des activités globales de management du risque d'un organisme..*

# 1.7 Management du risque lié à l'IA

## Liste des activités

1.7.1

Périmètre, contexte et critères

1.7.6

Approbation du plan de traitement du risque IA

1.7.2

Identification du risque

1.7.7

Communication et consultation

1.7.3

Analyse du risque

1.7.8

Enregistrement et élaboration de rapports

1.7.4

Évaluation du risque

1.7.9

Surveillance et revue

1.7.5

Traitement du risque

PECB

87

## 1.7.1 Périmètre, contexte et critères

ISO/IEC 23894, article 6.3.1

*Outre les recommandations données dans l'ISO 31000:2018, 6.3.1, pour les organismes qui utilisent l'IA, il convient d'étendre le périmètre d'application du management du risque lié à l'IA, le contexte du processus de management du risque lié à l'IA et les critères permettant d'évaluer l'importance du risque pour étayer les processus décisionnels, afin d'identifier à quels endroits des systèmes d'IA sont en cours de développement ou d'utilisation au sein de l'organisme. Il convient qu'un tel inventaire du développement et de l'utilisation de l'IA soit documenté et inclus dans le processus de management du risque de l'organisme.*

PECB

88

### **ISO31000, article6.3.1 Généralités**

*L'établissement du périmètre d'application, du contexte et des critères a pour but d'adapter le processus de management du risque, en permettant une appréciation du risque efficace et un traitement du risque approprié.*

*Le périmètre d'application, le contexte et les critères impliquent de définir le périmètre d'application du processus et de comprendre le contexte interne et externe.*

# Considération lors de l'établissement du contexte externe d'un organisme

## ISO/IEC 23894, Tableau 2

*Les recommandations données dans l'ISO 31000:2018, 5.4.1, s'appliquent.*

*Il convient que les organismes considèrent au moins les éléments suivants de leur contexte externe:*

- facteurs sociaux, culturels, politiques, légaux, réglementaires, financiers, technologiques, économiques et environnementaux, au niveau international, national, régional ou local;

- moteurs et tendances clés ayant une incidence sur les objectifs de l'organisme;

- relations avec les parties prenantes externes, leurs perceptions, leurs valeurs, leurs besoins et leurs attentes;

*Recommandations additionnelles pour les organismes engagés dans l'IA*

*Il convient que les organismes considèrent également, sans s'y limiter, les éléments suivants:*

- exigences légales pertinentes, y compris celles qui sont spécifiquement relatives à l'IA;

- lignes directrices sur l'utilisation et la conception éthiques de systèmes automatisés et d'IA publiées par des groupes liés au gouvernement, des organismes de régulation, des organismes de normalisation, des sociétés civiles, des académies et des associations industrielles;

- lignes directrices et cadres organisationnels spécifiques au domaine pour l'IA;

- tendances et avancées technologiques dans les différents domaines de l'IA;

- implications sociétales et politiques du déploiement de systèmes d'IA, y compris les recommandations issues des sciences sociales;

- perceptions des parties prenantes, qui peuvent être affectées par des enjeux tels que le manque de transparence (également opacité) des systèmes d'IA ou des systèmes d'IA biaisés;

- attentes des parties prenantes sur la disponibilité de solutions spécifiques basées sur l'IA et les moyens par lesquels les modèles d'IA sont mis à disposition (par exemple, par l'interface utilisateur ou par un kit de développement logiciel);

# Considération lors de l'établissement du contexte externe d'un organisme (suite)

ISO/IEC 23894, Tableau 2

<b>Les recommandations données dans l'ISO 31000:2018, 5.4.1, s'appliquent. Il convient que les organismes considèrent au moins les éléments suivants de leur contexte externe:</b>	<b>Recommandations additionnelles pour les organismes engagés dans l'IA Il convient que les organismes considèrent également, sans s'y limiter, les éléments suivants:</b>
<ul style="list-style-type: none"><li>— relations contractuelles et engagements;</li></ul>	<ul style="list-style-type: none"><li>— incidence de l'utilisation de l'IA, en particulier de systèmes d'IA utilisant l'apprentissage continu, sur la capacité de l'organisme à respecter ses obligations et garanties contractuelles. De ce fait, il convient que les organismes examinent attentivement la portée des contrats concernés;</li><li>— relations contractuelles établies pendant la conception et la production de systèmes ou services d'IA. Par exemple, il convient que les droits de propriété et d'utilisation des données d'essai et d'entraînement soient pris en compte lorsqu'ils sont fournis par des parties tierces;</li></ul>
<ul style="list-style-type: none"><li>— complexité des réseaux et des dépendances;</li></ul>	<ul style="list-style-type: none"><li>— l'utilisation de l'IA peut accroître la complexité des réseaux et des dépendances;</li></ul>
<ul style="list-style-type: none"><li>— (recommandations au-delà de l'ISO 31000:2018);</li></ul>	<ul style="list-style-type: none"><li>— un système d'IA peut remplacer un système existant et, dans un tel cas, une appréciation des avantages relatifs au risque et des transferts de risque d'un système d'IA par rapport à ceux du système existant peut être réalisée, en tenant compte des enjeux de sûreté ainsi que des environnementaux, sociaux, techniques et financiers associés à la mise en œuvre du système d'IA.</li></ul>

PECB

90

# Considération lors de l'établissement du contexte interne d'un organisme

ISO/IEC 23894, Tableau 3

<i>Les recommandations données dans l'ISO 31000:2018, 5.4.1, s'appliquent. Il convient que les organismes considèrent au moins les éléments suivants de leur contexte externe:</i>	<i>Recommandations additionnelles pour les organismes engagés dans l'IA Il convient que les organismes considèrent également, sans s'y limiter, les éléments suivants:</i>
— vision, mission et valeurs;	— aucune recommandation spécifique au-delà de l'ISO 31000:2018;
— gouvernance, organisation, rôles et responsabilités;	— aucune recommandation spécifique au-delà de l'ISO 31000:2018;
— stratégie, objectifs et politiques;	— aucune recommandation spécifique au-delà de l'ISO 31000:2018;
— culture de l'organisme;	— effet qu'un système d'IA peut avoir sur la culture de l'organisme en modifiant et en introduisant de nouveaux rôles, responsabilités et tâches;
— normes, lignes directrices et modèles adoptés par l'organisme;	— toute norme et ligne directrice locale, régionale, nationale et internationale additionnelle imposée par l'utilisation de systèmes d'IA;
— capacités, en termes de ressources et de connaissances (par exemple capital, temps, personnel, propriété intellectuelle, processus, systèmes et technologies);	— risques additionnels pour les connaissances de l'organisme par rapport à la transparence et à l'explicabilité des systèmes d'IA; — l'utilisation de systèmes d'IA peut entraîner des modifications dans le nombre de ressources humaines nécessaires pour réaliser une certaine capacité ou une variation du type de ressources nécessaires, par exemple, lors d'une perte de compétences ou d'expertise lorsque le processus humain de prise de décisions est de plus en plus soutenu par des systèmes d'IA;

PECB

91

# Considération lors de l'établissement du contexte interne d'un organisme (suite)

ISO/IEC 23894, Tableau 3

<b>Les recommandations données dans l'ISO 31000:2018, 5.4.1, s'appliquent.</b> Il convient que les organismes considèrent au moins les éléments suivants de leur contexte externe:	<b>Recommandations additionnelles pour les organismes engagés dans l'IA</b> Il convient que les organismes considèrent également, sans s'y limiter, les éléments suivants:
<ul style="list-style-type: none"><li>— données, systèmes d'information et circulation de l'information;</li></ul>	<ul style="list-style-type: none"><li>— connaissances spécifiques dans les technologies de l'IA et la science des données exigées pour développer et utiliser des systèmes d'IA;</li><li>— la disponibilité d'outils, de plateformes et de bibliothèques d'IA peut permettre le développement de systèmes d'IA sans que la technologie, ses limites et ses dangers potentiels soient complètement compris;</li><li>— potentiel de l'IA à soulever des enjeux et opportunités liés à la propriété intellectuelle pour des systèmes d'IA spécifiques, considération de leur propre propriété intellectuelle dans ce domaine, ainsi que les façons dont la propriété intellectuelle peut influencer la transparence, la sécurité et la capacité à collaborer avec les parties prenantes, afin de déterminer les étapes qu'il y a lieu de mettre en œuvre;</li><li>— des systèmes d'IA peuvent être utilisés pour automatiser, optimiser et améliorer le traitement des données;</li><li>— en tant que consommateurs de données, les systèmes d'IA peuvent se voir imposer des contraintes de qualité et de complétude additionnelles relatives aux données et aux informations;</li></ul>

PECB

92

# Considération lors de l'établissement du contexte interne d'un organisme (suite)

ISO/IEC 23894, Tableau 3

<i>Les recommandations données dans l'ISO 31000:2018, 5.4.1, s'appliquent. Il convient que les organismes considèrent au moins les éléments suivants de leur contexte externe:</i>	<i>Recommandations additionnelles pour les organismes engagés dans l'IA Il convient que les organismes considèrent également, sans s'y limiter, les éléments suivants:</i>
<ul style="list-style-type: none"><li>— relations avec les parties prenantes internes, en tenant compte de leurs perceptions et de leurs valeurs;</li></ul>	<ul style="list-style-type: none"><li>— perception des parties prenantes, qui peut être affectée par des enjeux tels que le manque de transparence des systèmes d'IA ou des systèmes d'IA biaisés.</li><li>— les besoins et attentes des parties prenantes peuvent être satisfaits dans une plus grande mesure par des systèmes d'IA spécifiques.</li><li>— besoin de la part des parties prenantes d'être formées aux capacités, modes de défaillance et management des défaillances des systèmes d'IA.</li></ul>
<ul style="list-style-type: none"><li>— relations contractuelles et engagements;</li></ul>	<ul style="list-style-type: none"><li>— perception des parties prenantes, qui peut être affectée par différents défis associés aux systèmes d'IA, tels que le manque potentiel de transparence et d'équité.</li><li>— les besoins et attentes des parties prenantes peuvent être satisfaits par des systèmes d'IA spécifiques.</li><li>— besoin de la part des parties prenantes d'être formées aux capacités, modes de défaillance et management des défaillances des systèmes d'IA.</li><li>— attentes des parties prenantes en matière de confidentialité, de droits fondamentaux individuels et collectifs et de libertés.</li></ul>
<ul style="list-style-type: none"><li>— interdépendances et interconnexions;</li></ul>	<ul style="list-style-type: none"><li>— l'utilisation de systèmes d'IA peut accroître la complexité des interdépendances et des interconnexions.</li></ul>

PECB

93

# Définition du périmètre d'application

## ISO/IEC 23894, article 6.3.2

*Les recommandations données dans l'ISO 31000:2018, 6.3.2, s'appliquent.*

*Il convient que le périmètre d'application tienne compte des tâches et responsabilités spécifiques des différents niveaux d'un organisme. En outre, il convient de prendre en considération les objectifs et buts des systèmes d'IA développés ou utilisés par l'organisme.*



PECB

94

### **ISO31000, article6.3.2 Définition du domaine d'application**

*Il convient que l'organisme définit le périmètre d'application de ses activités de management du risque.*

*Le processus de management du risque pouvant être appliqué à différents niveaux (par exemple au niveau de la stratégie, des opérations, d'un programme, d'un projet ou d'autres activités), il est important d'être précis quant au domaine d'application considéré, aux objectifs pertinents à prendre en compte et à leur alignement sur les objectifs de l'organisme.*

*Lors de la planification de l'approche, les éléments à prendre en compte comprennent:*

- *les objectifs et les décisions à prendre;*
- *les résultats attendus des étapes du processus;*
- *le temps, l'emplacement, les inclusions et exclusions spécifiques;*
- *les outils et techniques appropriés d'appréciation du risque;*
- *les ressources nécessaires, les responsabilités et la documentation à établir;*
- *les relations avec d'autres projets, processus et activités.*

# Définir les objectifs



Globalement, au niveau de l'organisme, le management du risque peut avoir les objectifs suivants :

- Garantir la conformité de l'organisme avec les exigences légales, réglementaires et contractuelles
- Faire preuve de « diligence raisonnable »
- Soutenir la prise de décision relative à l'orientation stratégique de l'organisme
- Identifier, analyser et traiter les risques lors de la conception et du développement de nouveaux produits et services



Pour des projets spécifiques, le management du risque peut avoir les objectifs suivants :

- Se conformer aux exigences légales, contractuelles et réglementaires
- Préparer un plan de réponse aux incidents
- Préparer un plan pour assurer la continuité d'activité
- Établir les prérequis d'un projet

PECB

95

Les objectifs d'un management du risque traduisent l'intention de l'organisme de traiter les risques identifiés et de se conformer aux exigences fixées. Il est important de déterminer clairement ces objectifs avec les parties prenantes concernées de l'organisme.

Les objectifs de management du risque sont nécessaires pour déterminer le périmètre et doivent être validés au plus haut niveau de l'organisme. Il convient donc d'identifier pour chaque projet des objectifs spécifiques qui formaliseront tous les éléments nécessaires à l'approbation de la direction. Les objectifs doivent être correctement documentés.

# Objectifs d'IA

## ISO/IEC 42001, Annexe C

### C.2.1 Redevabilité

*L'utilisation de l'IA peut modifier les cadres de redevabilité existants. Lorsque dans le passé des personnes réalisaient des actions pour lesquelles elles pouvaient être tenues responsables, de telles actions peuvent aujourd'hui être réalisées en tout ou partie par des systèmes d'IA.*

### C.2.2 Expertise en IA

*Une sélection de spécialistes dédiés dotés d'un ensemble de compétences et d'une expertise interdisciplinaires dans l'évaluation, le développement et le déploiement de systèmes d'IA est nécessaire.*

### C.2.3 Disponibilité et qualité des données d'essai et d'entraînement

*Les systèmes d'IA fondés sur l'apprentissage automatique ont besoin de données d'essai et d'entraînement pour les entraîner et vérifier leur comportement prévu.*

### C.2.4 Impact environnemental

*L'utilisation de l'IA peut avoir des impacts positifs et négatifs sur l'environnement.*

### C.2.5 Équité

*L'utilisation de l'IA pour la prise automatisée de décisions peut manquer d'équité pour des personnes ou groupes de personnes spécifiques.*

### C.2.6 Maintenabilité

*La maintenabilité a trait à la capacité de l'organisme à gérer les modifications du système d'IA afin de corriger des défauts ou de s'adapter à de nouvelles exigences.*

PECB

96

## ISO/IEC42001, article C.1 Généralités

Cette annexe présente les objectifs possibles de l'organisme, ainsi que les sources et les descriptions de risques qui peuvent être considérées par l'organisme pour son management du risque. Cette annexe n'a pas pour but d'être exhaustive ou de s'appliquer à tous les organismes. Il convient que l'organisme détermine les objectifs et les sources de risque pertinents pour son contexte. La norme ISO/IEC23894 fournit des informations plus détaillées sur ces objectifs et sources de risque, ainsi que sur leur lien avec le management du risque. Une évaluation initiale, régulière et en cas de nécessité des systèmes d'IA fournit la preuve qu'un système d'IA est évalué par rapport aux objectifs organisationnels.

# Objectifs d'IA (suite)

## ISO/IEC 42001, Annexe C

C.2.7 Respect de la vie privée	<p>L'utilisation incorrecte ou la divulgation de certaines données, en particulier des données à caractère personnel et des données sensibles (par exemple, dossiers médicaux) peut avoir des effets néfastes sur les personnes concernées.</p>
C.2.8 Robustesse	<p>Dans le domaine de l'IA, les propriétés de robustesse démontrent la capacité (ou l'incapacité) du système à maintenir un niveau de performance comparable aussi bien sur de nouvelles données que sur les données sur lesquelles il a été entraîné ou sur les données d'opérations courantes.</p>
C.2.9 Sûreté	<p>La sûreté a trait à l'attente qu'un système ne puisse, dans des circonstances définies, aboutir à un état dans lequel la vie humaine, la santé, la propriété ou l'environnement est mis en danger.</p>
C.2.10 Sécurité	<p>Dans le contexte de l'IA, et en particulier eu égard aux systèmes d'IA fondés sur des approches d'apprentissage automatique, il convient que de nouveaux enjeux de sécurité soient considérés au-delà des préoccupations classiques relatives à la sécurité de l'information et des systèmes.</p>
C.2.11 Transparence et explicabilité	<p>La transparence a trait à la fois aux caractéristiques d'un organisme exécutant des systèmes d'IA et à ces systèmes eux-mêmes. L'explicabilité a trait à la capacité d'expliquer aux parties intéressées les facteurs importants qui influencent les résultats du système d'IA d'une manière compréhensible pour les humains.</p>

PECB

97

# Objectifs S.M.A.R.T

La norme IEC 31010 recommande d'élaborer des objectifs S.M.A.R.T.  
pour manager les risques.



PECB

98

**Spécifique:** Comme le décrit la norme IEC31010, les objectifs devraient être spécifiques à l'objet de l'appréciation, c'est-à-dire au niveau auquel le processus de management du risque est appliqué (stratégique, opérationnel, programme, projet, etc.). Il convient que les objectifs soient bien définis, c'est-à-dire qu'ils soient explicites et ne laissent pas de place à des interprétations erronées. Les questions suivantes peuvent contribuer à l'élaboration d'objectifs spécifiques:

- Que faut-il faire?
- Quel est le résultat?
- Quelle est la fonction responsable au sein de l'organisme?
- D'autres parties prenantes doivent-elles être impliquées? Si oui, lesquelles?
- Pourquoi cet objectif est-il important?
- Existe-t-il des exigences à respecter?
- Existe-t-il des contraintes susceptibles d'empêcher la réalisation de l'objectif?

**Mesurable:** Il convient que l'organisme suive les progrès et mesure les résultats. Une déclaration d'objectifs pertinente devrait répondre aux questions suivantes: «quelles quantités, quelles ressources ou quels résultats.» L'organisme devrait également être capable de savoir si les objectifs sont réalisables et de mesurer leurs progrès. En général, les objectifs sont quantifiables, ce qui les rend relativement faciles à mesurer. Les objectifs qualitatifs, en revanche, peuvent représenter un défi plus important, car leurs résultats peuvent être interprétés de manière plus subjective. Dans ce cas, il convient de définir les critères comportementaux ou les preuves qui indiquent que l'objectif a été atteint.

**Atteignable:** Bien que des objectifs ambitieux et stimulants soient souvent souhaités, il convient que les objectifs soient atteignables dans le cadre des contraintes imposées par le contexte, comme décrit dans la norme IEC31010. Les questions qui peuvent être utiles à cette étape sont les suivantes:

- Est-il possible d'atteindre cet objectif?
- Les limites et les contraintes sont-elles connues?
- Disposons-nous des compétences nécessaires pour atteindre cet objectif?
- Cet objectif peut-il être atteint dans le délai imparti?

# Page de notes

---

PECB

99

**Réaliste:** Il convient que les objectifs soient pertinents par rapport aux objectifs organisationnels plus globaux, au contexte et au périmètre des activités de management du risque. À cette étape, il est également important de s'assurer de l'absence d'objectifs contradictoires.

**Temporel:** Il convient que les objectifs aient un délai de réalisation défini. Le fait de disposer d'un délai permettra à l'organisme de surveiller l'avancement de la réalisation des objectifs. Une simple question peut être utile à cette étape:

- Quand cet objectif sera-t-il atteint?

# Établir le contexte du processus de management du risque

## ISO/IEC 23894, article 6.3.3

*Les recommandations données dans l'ISO 31000:2018, 6.3.3, s'appliquent.*

*En raison de l'importance des effets potentiels des systèmes d'IA, il convient que l'organisme accorde une attention spécifique à l'environnement de ses parties prenantes lors de l'élaboration et de l'établissement du contexte du processus de management du risque.*



PECB

100

### **ISO/IEC23894, article6.3.3 Contexte interne et externe (suite)**

*Il convient de considérer soigneusement la liste des parties prenantes, y compris, sans s'y limiter:*

- *l'organisme (lui-même);*
- *les clients, les partenaires et les tierces parties;*
- *les fournisseurs;*
- *les utilisateurs finaux;*
- *les autorités de réglementation;*
- *les organisations civiles;*
- *les individus;*
- *les communautés concernées;*
- *les sociétés.*

*D'autres éléments à prendre en compte pour le contexte interne et externe sont les suivants:*

- *si les systèmes d'IA peuvent nuire aux êtres humains, s'opposer à des services essentiels (qui, s'ils étaient interrompus, mettraient en péril la vie, la santé ou la sûreté) ou enfreindre les droits de l'homme (par exemple, par une prise de décision automatisée biaisée et manquant d'équité) ou contribuer à nuire à l'environnement;*
- *attentes internes et externes relatives à la responsabilité sociétale de l'organisme;*
- *attentes internes et externes relatives à la responsabilité environnementale de l'organisme.*

*Il convient que les lignes directrices de l'ISO26000:2010 soulignant des aspects de la responsabilité sociétale s'appliquent en tant que cadre pour comprendre et traiter le risque, en particulier sur des sujets fondamentaux relatifs à la gouvernance de l'organisme, aux droits de l'homme, aux relations et conditions de travail, à l'environnement, à la loyauté des pratiques, aux questions relatives aux consommateurs et aux communautés ainsi qu'au développement local.*

# Établir le contexte du processus de management du risque

- Lors de la conception du cadre de management du risque, le contexte est analysé à l'échelle de l'organisme afin de s'assurer que les politiques, les procédures et les rôles (à savoir les fondements) sont correctement établis et adaptés aux besoins de l'organisme.
- Après avoir établi le contexte du processus de management du risque, le but est de s'assurer que l'organisme comprend bien l'*objet* de l'appréciation, qui peut par exemple être une nouvelle activité, une nouvelle stratégie, un projet, un programme, un partenariat potentiel, etc. Comme décrit dans la norme ISO 31000, le processus de management du risque peut être appliqué à différents niveaux (stratégique, tactique, opérationnel).

PECB

101

Les informations de contexte de l'organisme obtenues lors de l'établissement du cadre (parties prenantes, obligations de conformité, culture, relations contractuelles, etc.) peuvent être utilisées pour établir le contexte du processus de management du risque.

## ***ISO31000, article6.3.3 Contexte interne et externe***

*Le contexte interne et externe est l'environnement dans lequel l'organisme cherche à définir et atteindre ses objectifs. Il convient que le contexte du processus de management du risque soit établi à partir de la compréhension de l'environnement externe et interne dans lequel opère l'organisme et qu'il reflète l'environnement spécifique de l'activité à laquelle le processus de management du risque doit être appliqué. La compréhension du contexte est importante car:*

- *le management du risque a lieu dans le contexte des objectifs et des activités de l'organisme;*
- *les facteurs organisationnels peuvent être une source de risque;*
- *la finalité et le domaine d'application du processus de management du risque peuvent être corrélés aux objectifs de l'organisme dans son ensemble.*

Les questions suivantes peuvent contribuer à établir le contexte du processus de management du risque:

- Quels sont la politique, le programme, le processus, l'activité, la procédure et le projet?
- Qui sont les parties prenantes?
- Quels sont les indicateurs clés de performance (ICP)?
- Quels sont les principaux indicateurs de risque?
- Quels sont les principaux résultats attendus?
- Quels sont les facteurs importants au sein de l'organisme qui ont un impact sur ce domaine, par exemple, les attentes opérationnelles, environnementales, sociétales, communautaires et technologiques?
- Quels ont été les problèmes identifiés lors des revues précédentes?
- Quelles sont les considérations en matière de coûts et de revenus?

# Définir les critères de risque

## ISO/IEC 23894, Tableau 4

<b>Considérations pour la définition des critères de risque, tel que donné dans l'ISO 31000:2018, 6.3.4</b>	<b>Considérations additionnelles dans le contexte du développement et de l'utilisation de systèmes d'IA</b>
— Nature et type des incertitudes pouvant avoir une incidence sur les conséquences et les objectifs (tangibles et intangibles).	— Il convient que les organismes mettent en œuvre des étapes raisonnables pour comprendre l'incertitude dans toutes les parties du système d'IA, y compris les données utilisées, les logiciels, les modèles mathématiques, l'extension physique et les aspects liés aux interventions humaines du système (tels que toute activité humaine relative à la collecte et l'étiquetage des données).
— Façon dont les conséquences (positives et négatives) et la vraisemblance sont définies et mesurées.	— aucune recommandation spécifique au-delà de l'ISO 31000:2018.
— Facteurs liés au temps.	
— Cohérence dans l'utilisation des mesures.	— Il convient que les organismes soient conscients que l'IA est un domaine technologique qui évolue rapidement. Il convient que les méthodes de mesure soient évaluées de manière cohérente en fonction de leur efficacité et de leur pertinence pour les systèmes d'IA utilisés.
— Méthode de détermination du niveau de risque.	— Il convient que les organismes établissent une approche cohérente pour déterminer le niveau de risque. Il convient que l'approche reflète l'impact potentiel des systèmes d'IA eu égard aux différents objectifs liés à l'IA.

102

### ISO/IEC23894, article6.3.4 Définition des critères de risque

Les recommandations données dans l'ISO31000:2018, 6.3.4, s'appliquent.

Outre les recommandations données dans l'ISO31000:2018, 6.3.4, le Tableau4 fournit des lignes directrices additionnelles sur les facteurs à prendre en considération lors de la définition des critères de risque.

### ISO31000, article6.3.4 Définition des critères de risque

Il convient que l'organisme spécifie le niveau et le type de risque pouvant ou non être pris par l'organisme, en fonction des objectifs. Il convient également qu'il définisse des critères permettant d'évaluer l'importance du risque et d'étayer les processus décisionnels. Il convient que les critères de risque soient alignés sur le cadre organisationnel de management du risque et adaptés à la finalité et au domaine d'application spécifique de l'activité considérée. Il convient que les critères de risque reflètent les valeurs, les objectifs et les ressources de l'organisme et soient cohérents avec les politiques et déclarations en matière de management du risque. Il convient que les critères soient définis en tenant compte des obligations de l'organisme et de l'opinion des parties prenantes.

Bien qu'il convienne d'établir les critères de risque au début du processus d'appréciation du risque, ces critères sont dynamiques et il convient qu'ils soient revus en permanence et modifiés si nécessaire.

# Définition des critères de risque (suite)

## ISO/IEC 23894, Tableau 4

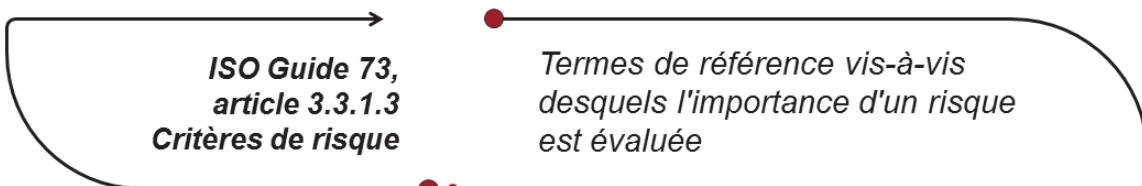
<b>Considérations pour la définition des critères de risque, tel que donné dans l'ISO 31000:2018, 6.3.4</b>	<b>Considérations additionnelles dans le contexte du développement et de l'utilisation de systèmes d'IA</b>
<ul style="list-style-type: none"><li>— Façon dont les combinaisons et séquences de plusieurs risques seront prises en compte.</li></ul>	<ul style="list-style-type: none"><li>— aucune recommandation spécifique au-delà de l'ISO 31000:2018.</li></ul>
<ul style="list-style-type: none"><li>— Capacité de l'organisme.</li></ul>	<ul style="list-style-type: none"><li>— Il convient que la capacité en IA, le niveau de connaissance et la capacité à atténuer les risques concrets liés à l'IA soient pris en compte lors de la définition du goût du risque lié à l'IA.</li></ul>

# Définir les critères de risque

## ISO 31000, article 6.3.4

*Il convient que l'organisme spécifie le niveau et le type de risque pouvant ou non être pris par l'organisme, en fonction des objectifs. Il convient également qu'il définisse des critères permettant d'évaluer l'importance du risque et d'étayer les processus décisionnels.*

*Il convient que les critères de risque soient alignés sur le cadre organisationnel de management du risque et adaptés à la finalité et au domaine d'application spécifique de l'activité considérée.*



PECB

104

## ISO/IEC31000, article6.3.4 Définition des critères de risque (suite)

Pour fixer les critères de risque, il convient de prendre en compte les éléments suivants:

- la nature et le type d'incertitudes pouvant avoir une incidence sur les résultats et les objectifs (tangibles et intangibles);
- la façon dont les conséquences (positives et négatives) et la vraisemblance seront définies et mesurées;
- facteurs liés au temps;
- la cohérence dans l'utilisation des mesures;
- la méthode de détermination du niveau de risque;
- la façon dont les combinaisons et séquences de plusieurs risques seront prises en compte;
- la capacité de l'organisme.

## 1.7.2 Identification du risque

ISO 31000, article 6.4.2

*Il est essentiel que les informations utilisées pour l'identification du risque soient pertinentes, appropriées et à jour.*

*Il convient que l'organisme identifie les risques, que leurs sources soient ou non sous son contrôle. Il convient de tenir compte du fait qu'il peut y avoir plusieurs types de résultats pouvant avoir diverses conséquences tangibles ou intangibles.*

PECB

105

### ISO/IEC23894, article6.4.2.1 Généralités

Les recommandations données dans l'ISO31000:2018, 6.4.2, s'appliquent.

### IEC31010, article6.3.2 Identification du risque

*L'identification du risque permet une prise en compte explicite de l'incertitude. Toutes les sources d'incertitudes et les effets tant bénéfiques que néfastes peuvent être pertinents, en fonction du contexte et du domaine d'application de l'appréciation.*

*Les techniques d'identification du risque s'appuient en général sur les connaissances et l'expérience d'un certain nombre de parties prenantes. Il s'agit notamment de savoir:*

- quelle incertitude existe et quels peuvent être ses effets;
- quelles circonstances ou quels problèmes (tangibles ou intangibles) sont susceptibles de présenter des conséquences futures;
- quelles sources de risques sont présentes ou peuvent apparaître;
- quels moyens de maîtrise sont en place et s'ils sont efficaces;
- quels événements et conséquences peuvent se produire, et comment, quand, où et pourquoi;
- ce qu'il s'est passé et comment cela peut être raisonnablement associé au futur;
- quels aspects humains et facteurs organisationnels pourraient s'appliquer.

*Des enquêtes physiques peuvent également être utiles pour identifier les sources de risques ou les signes précurseurs d'éventuelles conséquences.*

*Le résultat de l'identification du risque peut être consigné sous la forme d'une liste de risques avec les événements, les causes et les conséquences spécifiés, ou en utilisant d'autres formats.*

*Quelles que soient les techniques utilisées, il convient d'appréhender l'identification du risque de manière méthodique et itérative de sorte qu'elle soit complète et efficace. Il convient dans la mesure du possible d'identifier le risque suffisamment tôt pour permettre la prise de mesures. Il arrive cependant que certains risques ne puissent pas être identifiés au cours d'une appréciation du risque. Il convient donc de mettre en place un mécanisme pour recueillir les risques émergents et reconnaître les signes précurseurs d'une réussite ou d'un échec potentiel(le).*

# Identification des actifs

## ISO/IEC 23894, article 6.4.2.2

*Il convient que l'organisme identifie les actifs relatifs à la conception et à l'utilisation de l'IA qui relèvent de la portée du processus de management du risque. La compréhension des actifs relevant de la portée du processus et de la criticité ou valeur relative de ces actifs fait partie intégrante de l'appréciation de l'impact. Il convient que la valeur et la nature de l'actif (tangible ou intangible) soient considérées.*



PECB

106

### ISO/IEC 23894, article 6.4.2.2 Identification des actifs et de leur valeur (suite)

*De plus, en relation avec le développement et l'utilisation de l'IA, il convient que les actifs soient considérés dans le contexte des éléments suivants, sans s'y limiter:*

- **actifs de l'organisme et leur valeur:**
  - les actifs tangibles peuvent inclure les données, les modèles et le système d'IA lui-même;
  - les actifs intangibles peuvent inclure la réputation et la confiance;
- **actifs des individus et leur valeur:**
  - les actifs tangibles peuvent inclure les données à caractère personnel des individus;
  - les actifs intangibles peuvent inclure le respect de la vie privée, la santé et la sûreté d'un individu;
- **actifs et valeurs pour les communautés et sociétés:**
  - les actifs tangibles peuvent inclure l'environnement;
  - les actifs intangibles sont susceptibles de reposer davantage sur des valeurs, telles que les croyances socioculturelles, les connaissances des communautés, l'accès à l'éducation et l'équité.

### ISO 55000, article 2.3 Actifs

*Un actif est considéré comme un item, une chose ou une entité qui a une valeur potentielle ou réelle pour un organisme. Cette valeur varie selon les organismes et leurs parties prenantes et peut être matérielle ou immatérielle, financière ou non financière.*

*La période allant de la création d'un actif à la fin de sa vie est la durée de vie de l'actif. La durée de vie d'un actif ne coïncide pas nécessairement avec la période pendant laquelle un organisme en est responsable; au contraire, un actif peut fournir une valeur potentielle ou réelle à un ou plusieurs organismes pendant sa durée de vie, et la valeur de l'actif pour un organisme peut changer au cours de sa durée de vie.*

Afin d'identifier les actifs, il convient d'examiner le périmètre de l'appréciation du risque et d'identifier les actifs entrant dans ce périmètre. Une liste des actifs à gérer et une liste des processus opérationnels liés aux actifs et à leur pertinence seront générées en sortie.

# Types d'actifs

Le niveau de détail utilisé lors de l'identification des actifs a un effet essentiel sur la quantité d'informations collectées lors de l'appréciation du risque. Il existe deux types d'actifs :

## Actifs primordiaux

- Processus opérationnels et activités
- Information

## Actifs en support

- |                                                                                                |                                                                                                                  |
|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Matériel</li><li>• Logiciel</li><li>• Réseau</li></ul> | <ul style="list-style-type: none"><li>• Personnel</li><li>• Site</li><li>• Structure organisationnelle</li></ul> |
|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|

# Inventaire des actifs

- Il convient que les organismes identifient et enregistrent leurs actifs dans un inventaire.
- Cet inventaire devrait contenir des informations sur le type d'actifs, leur taille, leur emplacement, leur propriétaire, les informations de sauvegarde et leur valeur pour l'organisme.
- L'inventaire des actifs devrait être précis, actualisé, cohérent et aligné avec les autres inventaires.
- L'inventaire des actifs est une composante importante du management des risques qui aide les organismes à assurer une protection adéquate de leurs actifs.

Tous les actifs qui font partie de cet inventaire devraient être sous la responsabilité d'un propriétaire. Le propriétaire de l'actif est responsable de sa gestion tout au long de son cycle de vie.



PECB

108

## **ISO/IEC27002, article 5.9 Inventaire des informations et autres actifs associés**

### **Objectif**

*Identifier les informations et autres actifs associés de l'organisation afin de préserver leur sécurité et d'en attribuer la propriété de manière appropriée.*

### **Recommandations**

*Il convient que l'organisation identifie ses informations et autres actifs associés et qu'elle détermine leur importance en termes de sécurité de l'information. Il convient que la documentation soit tenue à jour dans des inventaires dédiés ou déjà en place selon le cas.*

*Il convient que l'inventaire des informations et autres actifs associés soit correct, à jour, cohérent et aligné avec les autres inventaires. Les possibilités pour assurer l'exactitude d'un inventaire des informations et autres actifs associés incluent de:*

- a. mener des vérifications régulières des informations et autres actifs associés identifiés par rapport à l'inventaire des actifs;
- b. appliquer automatiquement une mise à jour de l'inventaire lors de l'installation, du changement ou retrait d'un actif.

*Il convient que l'emplacement de chaque actif soit indiqué dans l'inventaire au besoin.*

*Il n'est pas nécessaire que l'inventaire corresponde à une seule liste des informations et autres actifs associés. Compte tenu du fait qu'il convient que l'inventaire soit maintenu par les fonctions appropriées, il peut être considéré comme un ensemble d'inventaires dynamiques, tels que les inventaires d'actifs informationnels, de matériels, de logiciels, de machines virtuelles (VM), d'installations, de personnel, de compétences, de capacités et d'enregistrements.*

# Identification des sources de risques

## ISO/IEC 23894, article 6.4.2.3

*Il convient que l'organisme identifie une liste de sources de risques relatives au développement ou à l'utilisation de l'IA, ou les deux, au sein du périmètre d'application défini.*

*Ces sources de risques peuvent être identifiées dans les domaines suivants, sans s'y limiter:*

- organisme;
- processus et procédures;
- routines de management;
- personnel;
- environnement physique;
- données;
- configuration du système d'IA;
- environnement de déploiement;
- équipements matériels, logiciels, ressources réseau et services;
- dépendance à des parties externes.

PECB

109

# Sources de risque

## ISO/IEC 42001, Annexe C.3

### C.3.1 Complexité de l'environnement

Lorsque les systèmes d'IA fonctionnent dans des environnements complexes, où l'éventail des situations est important, il peut y avoir une incertitude sur les performances et donc une source de risque (par exemple, l'environnement complexe de la conduite autonome).

### C.3.2 Manque de transparence et d'explicabilité

L'incapacité à fournir des informations appropriées aux parties intéressées peut être une source de risque (c'est-à-dire en termes de fiabilité et de redevabilité de l'organisme).

### C.3.3 Niveau d'automatisation

Le niveau d'automatisation peut avoir un effet sur plusieurs domaines de préoccupation, tels que la sûreté, l'équité ou la sécurité.

### C.3.4 Sources de risques liés à l'apprentissage automatique

La qualité des données utilisées dans l'apprentissage automatique et le processus de collecte des données peuvent être des sources de risque, car ils peuvent avoir une incidence sur des objectifs tels que la sécurité et la robustesse (par exemple, en raison de problèmes de qualité des données ou d'empoisonnement des données).

# Sources de risque

ISO/IEC 42001, Annexe C.3

## C.3.5 Enjeux relatifs aux équipements matériels du système

Les sources de risque liées aux enjeux relatifs aux équipements matériels incluent les erreurs matérielles dues à des composants défectueux ou le transfert de modèles d'apprentissage automatique entraînés entre différents systèmes.

## C.3.6 Enjeux relatifs au cycle de vie du système

Des sources de risque peuvent apparaître tout au long du cycle de vie du système d'IA (par exemple, défauts de conception, déploiement inadéquat, manque de maintenance, problèmes de décommissionnement).

## C.3.7 Maturité de la technologie

Les sources de risque peuvent être liées à une technologie moins mature en raison de facteurs inconnus (par exemple, les contraintes du système et les conditions limites, la dérive des performances), mais aussi à une technologie plus mature pouvant engendrer un risque de complaisance technologique.

# Identification des événements et conséquences potentiels

## ISO/IEC 23894, article 6.4.2.4

*Il convient que l'organisme identifie les événements potentiels liés au développement ou à l'utilisation de l'IA et pouvant entraîner des conséquences tangibles ou intangibles variées.*

*Les événements peuvent être identifiés selon une ou plusieurs des méthodes et sources suivantes:*

- normes publiées;*
- spécifications techniques publiées;*
- rapports techniques publiés;*
- articles scientifiques publiés;*
- données du marché sur des systèmes ou applications similaires en cours d'utilisation;*
- rapports d'incidents sur des systèmes ou applications similaires en cours d'utilisation;*
- essais sur le terrain;*
- études d'usabilité;*
- résultats d'investigations appropriées;*
- rapports de parties prenantes;*
- entretiens avec des experts internes ou externes et rapports provenant de ceux-ci;*
- simulations.*

**PECB**

112

# Identification des mesures

## ISO/IEC 23894, article 6.4.2.5

*Il convient que l'organisme identifie les mesures pertinentes pour le développement ou l'utilisation de l'IA, ou les deux. Il convient d'identifier les mesures lors des activités de management du risque ainsi que de les documenter (dans les systèmes internes, les modes opératoires, les rapports d'audit, etc.).*

*Les mesures peuvent être utilisées pour avoir une incidence positive sur le risque global en atténuant les sources et événements de risques ainsi que leurs conséquences.*

*Il convient que l'efficacité opérationnelle des mesures identifiées soit prise en compte, en particulier les défaillances des mesures.*



PECB

113

# Identification des conséquences

## ISO/IEC 23894, article 6.4.2.6

Dans le cadre de l'appréciation du risque lié à l'IA, il convient que l'organisme identifie les sources de risques, événements ou conséquences qui peuvent entraîner des risques. Il convient également d'identifier les éventuelles conséquences pour l'organisme lui-même, ainsi que pour les personnes, communautés, groupes et sociétés. Il convient que les organismes prennent des précautions particulières pour identifier les différences entre les groupes qui bénéficient des avantages de la technologie et les groupes qui en subissent les conséquences négatives.

Les conséquences pour l'organisme sont nécessairement différentes de celles pour les individus et les sociétés. Les conséquences pour les organismes peuvent inclure, sans s'y limiter:

- délai d'investigation et de réparation;
- perte ou gain de temps (de travail);
- perte ou gain d'opportunités;
- menaces envers la santé ou la sûreté des individus;
- coûts financiers des compétences spécifiques pour réparer les dommages;

PECB

114

## ISO/IEC 23894, article 6.4.2.6 Identification des conséquences (suite)

- recrutement, satisfaction et fidélisation des employés;
- réputation et confiance;
- pénalités et amendes;
- litiges client.

Selon le contexte, les conséquences pour les individus et sociétés peuvent être plus générales, auquel cas il peut être impossible pour l'organisme d'estimer exactement quels sont les impacts pour chaque individu ou pour les sociétés.

Plutôt que de spécifier chaque type d'impact, cela peut être considéré de manière générale, le degré de criticité des impacts (par exemple, pour le respect de la vie privée, l'équité, les droits de l'homme, etc. dans le cas d'un individu, ou pour l'environnement dans le cas des sociétés) étant un élément clé.

Ces impacts exacts peuvent dépendre du contexte dans lequel l'organisme évolue et des domaines pour lesquels le système d'IA est développé et utilisé.

**NOTE1** Ces conséquences peuvent être positives ou négatives. L'organisme peut tenir compte de ses deux types de conséquences lors de l'appréciation des conséquences pour l'organisme, pour les individus et pour la société.

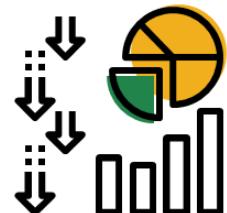
**NOTE2** Les conséquences pour les individus et les sociétés peuvent généralement aboutir également à des conséquences pour l'organisme. Par exemple, un incident de sûreté affectant l'utilisateur d'un produit de l'organisme peut aboutir à des mises en cause de sa responsabilité et avoir une incidence négative sur sa réputation et ses ventes de produits.

## 1.7.3 Analyse du risque

### ISO 31000, article 6.4.3

*Il convient que l'analyse du risque prenne en compte des facteurs tels que:*

- la vraisemblance des événements et des conséquences;
- la nature et l'importance des conséquences;
- la complexité et l'interconnexion;
- les facteurs liés au temps et la volatilité;
- l'efficacité des moyens de maîtrise existants;
- les niveaux de sensibilité et de confiance.



PECB

115

#### **ISO31000, article6.4.3 Analyse du risque (suite)**

*L'analyse du risque peut être influencée par toute divergence d'opinions, biais, perception du risque et jugement. Les influences supplémentaires sont la qualité des informations utilisées, les hypothèses et exclusions posées, toute limitation des techniques et la façon dont elles sont mises en œuvre. Il convient que ces influences soient prises en compte, documentées et communiquées aux décideurs.*

*Les événements extrêmement incertains peuvent être difficiles à quantifier. Cela peut poser problème lors de l'analyse d'événements ayant de graves conséquences. Dans de tels cas, l'utilisation d'une combinaison de techniques permet généralement d'acquérir une connaissance plus approfondie.*

*L'analyse du risque fournit des données permettant d'évaluer le risque, de prendre la décision de le traiter ou non et de quelle manière, et permet de choisir la stratégie et les méthodes de traitement les plus performantes. Les résultats fournissent des renseignements en vue des décisions quand il faut effectuer des choix et que les options impliquent différents types et niveaux de risque.*

#### **ISO/IEC23894, article6.4.3.1 Généralités**

*Les recommandations données dans l'ISO31000:2018, 6.4.3, s'appliquent.*

*Il convient que l'approche d'analyse soit cohérente avec les critères de risque élaborés dans le cadre de l'établissement du contexte.*

# Sélection d'une approche d'analyse du risque

ISO 31000, article 6.4.3

*L'analyse du risque peut être menée à différents niveaux de détail et de complexité selon la finalité de l'analyse, la disponibilité et la fiabilité des informations et les ressources disponibles.*

*Les techniques d'analyse peuvent être qualitatives, quantitatives, ou une combinaison de celles-ci, selon les circonstances et l'utilisation prévue.*



# Appréciation des conséquences

## ISO/IEC 23894, article 6.4.3.2

- Lors de l'appréciation des conséquences identifiées lors de l'appréciation du risque, il convient que l'organisme fasse la distinction entre une appréciation de l'impact pour l'organisme, une appréciation de l'impact pour les individus et une appréciation de l'impact pour la société.
- Il convient que les analyses d'impact pour l'organisme déterminent le degré auquel l'organisme est affecté et considèrent les éléments suivants, sans s'y limiter:
  - criticité de l'impact;
  - impacts tangibles et intangibles;
  - critères utilisés pour établir l'impact global.



PECB

117

### ISO/IEC 23894, article 6.4.3.2 Appréciation des conséquences (suite)

Il convient que les analyses d'impact pour les individus déterminent le degré auquel un individu peut être affecté par le développement ou l'utilisation de l'IA par l'organisme, ou les deux. Il convient qu'elles tiennent compte des éléments suivants, sans s'y limiter:

- types de données des individus utilisées;
- impact prévu du développement ou de l'utilisation de l'IA;
- impact potentiel du biais sur un individu;
- impact potentiel sur les droits fondamentaux, pouvant entraîner des dommages matériels et immatériels pour l'individu;
- impact potentiel de l'équité sur un individu;
- sûreté d'un individu;
- protections et mesures d'atténuation relatives au biais indésirable et au manque d'équité;
- environnement juridictionnel et culturel de l'individu (ce qui peut affecter la façon dont l'impact relatif est déterminé).

Il convient que les analyses d'impact pour les sociétés déterminent le degré auquel une société peut être affectée par le développement ou l'utilisation de l'IA par l'organisme, ou les deux. Il convient qu'elles tiennent compte des éléments suivants, sans s'y limiter:

- portée de l'impact sociétal (quelle est la portée du système d'IA au sein de différentes populations), y compris les personnes qui utilisent le système ou pour lesquelles il est conçu (par exemple, une utilisation gouvernementale peut potentiellement avoir une incidence sur les sociétés qui dépasse l'utilisation privée);
- la façon dont un système d'IA influence les valeurs sociales et culturelles des différents groupes concernés (y compris les façons spécifiques dont le système d'IA amplifie ou atténue les modèles de préjudice préexistants pour les différents groupes sociaux).

### IEC 31010, article 6.3.5.1 Analyse du type, de l'ampleur et de la durée des conséquences

L'analyse des conséquences peut s'étendre d'une simple description des résultats à une modélisation quantitative ou une analyse de vulnérabilité approfondie.

# Page de notes

---

PECB

118

## **IEC31010, article 6.3.5.1 Analyse du type, de l'ampleur et de la durée des conséquences (suite)**

*Il convient de prendre en considération les effets collatéraux (effets domino ou secondaires), lorsqu'une conséquence découle d'une autre.*

*Le risque peut être associé à un certain nombre de types de conséquences différents, qui ont un impact sur les différents objectifs. Il convient de choisir les types de conséquences à analyser au moment de la planification de l'appréciation. Il convient de vérifier les déclarations de contexte afin de s'assurer que les conséquences à analyser correspondent bien aux objectifs de l'appréciation et aux décisions à prendre. Cela peut être adapté au fil de l'appréciation à mesure de la disponibilité d'informations supplémentaires.*

# Analyser la vraisemblance

## Approches générales pour estimer la vraisemblance

Utiliser des données historiques pertinentes



Obtenir l'avis d'experts



Prévoir la probabilité



PECB

119

### **ISO/IE 23894, article 6.4.3.3 Appréciation de la vraisemblance**

*Le cas échéant, il convient que l'organisme apprécie la vraisemblance des événements et conséquences entraînant des risques. La vraisemblance peut être déterminée sur une échelle qualitative ou quantitative et il convient qu'elle s'aligne aux critères établis dans le cadre de 6.3.4. La vraisemblance peut affecter les éléments suivants et avoir une incidence sur ces derniers, sans s'y limiter:*

- types, importance et nombre de sources de risques;
- fréquence, sévérité et omniprésence des menaces;
- facteurs internes tels que la réussite opérationnelle des politiques et procédures, et la motivation des acteurs internes;
- facteurs externes tels que la géographie et autres préoccupations sociales, économiques et environnementales;
- réussite (atténuation) ou défaillance des mesures.

*Il convient que les organismes intègrent des calculs de vraisemblance uniquement lorsque ces derniers sont applicables et utiles à l'identification des niveaux où un traitement du risque doit être appliqué. Il peut exister des enjeux techniques, économiques et heuristiques significatifs avec les vraisemblances fondées sur la prise de décisions, en particulier lorsque la vraisemblance ne peut pas être calculée ou lorsque le calcul est associé à une grande marge d'erreur.*

### **IEC31010, article 6.3.5.2 Analyse de vraisemblance**

*La vraisemblance peut faire référence à la vraisemblance d'un événement ou à celle d'une conséquence spécifiée. Il convient d'établir explicitement le paramètre auquel s'applique une valeur de vraisemblance et il convient de définir précisément l'événement ou la conséquence dont la vraisemblance est en train d'être établie. Pour définir la vraisemblance de manière exhaustive, il peut être nécessaire d'inclure une déclaration concernant l'exposition et la durée.*

# Apprécier la vraisemblance

Exemple d'échelle qualitative utilisée par une entreprise de teinture textile

Vraisemblance	Probabilité	Exemple d'incident possible
1 – Rare	1 à 2 fois ou une fois pour 75 à 100 % de la période cible	La pollution de l'environnement se produit une fois tous les dix ans.
2 – Peu fréquent	1 à 3 fois ou une fois pour 50 à 70 % de la période cible	La technologie de teinture est modifiée une fois tous les cinq ans.
3 – Assez fréquent	3 à 5 fois ou une fois pour 25 à 50 % de la période cible	Des fusions et des acquisitions sont observées avec les sous-traitants trois fois en cinq ans.
4 – Fréquent	5 à 10 fois ou une fois pour 5 à 25 % de la période cible	Des contrefaçons des produits de l'entreprise sont observées neuf fois en cinq ans.
5 – Très fréquent	Plus de 10 fois ou une fois pour 0 à 5 % de la période cible	Les obligations contractuelles sont enfreintes 12 fois en trois ans.

PECB

120

Après avoir identifié les scénarios pertinents et avoir estimé leurs conséquences, il convient d'estimer la probabilité d'occurrence de chaque scénario. Il est nécessaire d'estimer la probabilité réaliste d'un incident et les impacts associés aux contrôles ou mesures déjà en place.

## **IEC31010, article6.3.5.2 Analyse de vraisemblance**

*EXEMPLE 1 La déclaration selon laquelle un fournisseur a 5 % de chance de ne pas assurer une livraison est vague tant en ce qui concerne la période de temps que la population. Il n'apparaît pas clairement non plus si le pourcentage concerne 5 % des projets ou 5 % des fournisseurs. Pour être plus explicite, la déclaration serait formulée de la manière suivante: "la probabilité qu'un ou que plusieurs fournisseurs n'assurent pas la livraison des marchandises ou des services exigés pendant la durée d'un projet est de 5 % des projets".*

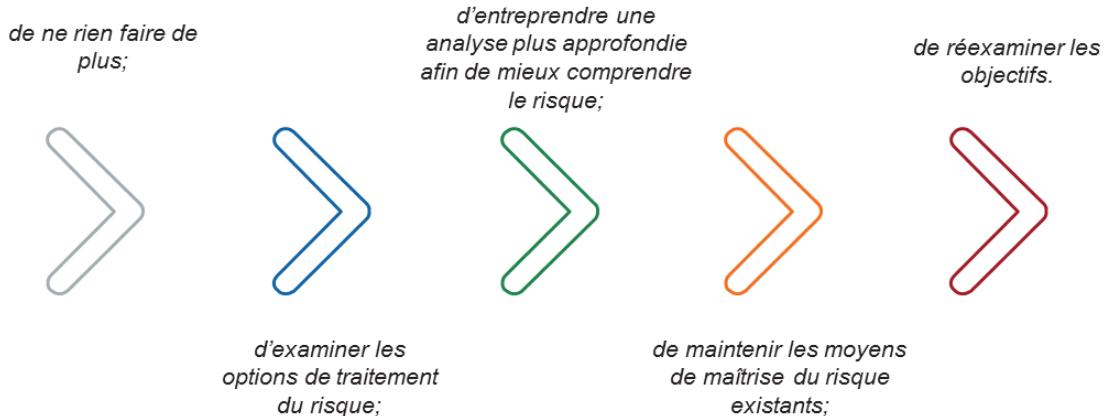
*Pour réduire le plus possible les mauvaises interprétations lors de l'expression d'une vraisemblance, de manière qualitative ou quantitative, il convient de préciser explicitement la période de temps et la population concernée dans le domaine d'application de l'appréciation.*

*EXEMPLE 2 La probabilité qu'un ou que plusieurs fournisseurs n'assurent pas la livraison des marchandises ou des services exigés par un projet dans les deux mois qui suivent est de 1 % des projets, alors que sur une période de six mois, une défaillance peut se produire dans 3 % des projets.*

# Évaluation du risque

## ISO 31000, article 6.4.4

L'évaluation du risque a pour but de déboucher sur des décisions plus judicieuses. L'évaluation du risque consiste à comparer les résultats de l'analyse du risque aux critères de risque établis afin de déterminer si une action supplémentaire est exigée. Cela peut déboucher sur la décision:



PECB

121

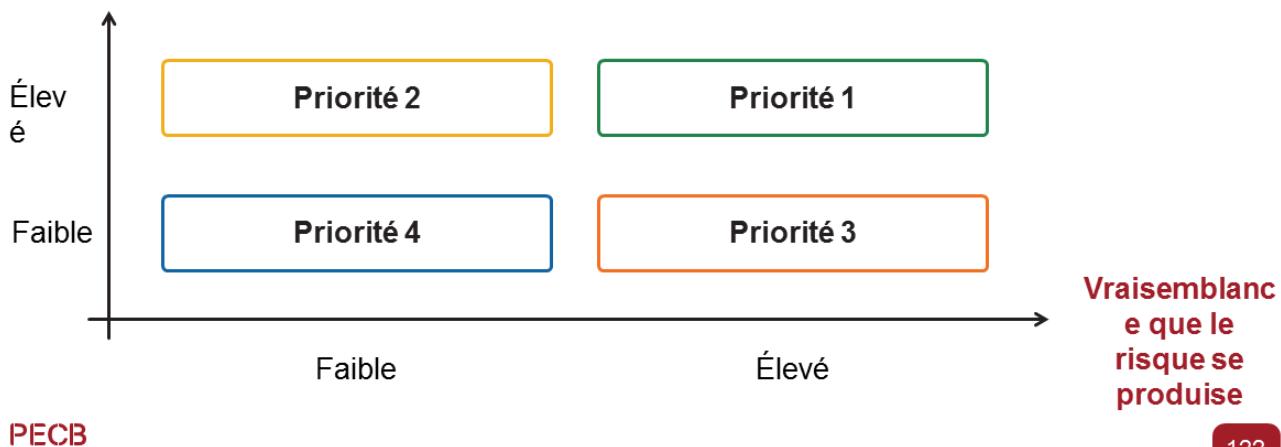
## ISO/IEC23894, article 6.4.4 Évaluation du risque

Les recommandations données dans l'ISO31000:2018, 6.4.4, s'appliquent.

# Priorisation des risques pour le traitement du risque

L'organisation doit hiérarchiser les risques afin de concentrer les efforts de traitement sur les risques qui ont à la fois un impact et une vraisemblance plus élevés.

## Impact du risque



Les organismes doivent hiérarchiser les risques afin de concentrer les efforts de traitement sur les risques qui ont à la fois un impact et une vraisemblance plus élevés. Il convient d'abord d'identifier les risques puis de les classer en fonction de leur priorité. Les risques sont ainsi gérés plus efficacement.

Le concept de risque zéro n'existe pas, mais il est possible de définir un seuil en dessous duquel le risque est acceptable pour l'organisme et aucune activité n'est entreprise pour réduire ce risque. D'autre part, il existe un seuil au-delà duquel le risque est inacceptable et sa source devrait être éliminée ou réduite.

La hiérarchisation des risques permet aux organismes de déterminer les actions à entreprendre pour traiter les risques en fonction de leur niveau.

## **ISO/IEC27005, article7.4.2 Classement des risques analysés par ordre de priorité en vue de leur traitement**

*L'évaluation du risque utilise la compréhension des risques obtenue par l'analyse du risque pour faire des propositions afin de décider de la prochaine étape à suivre. Il convient que celles-ci précisent:*

- si un traitement du risque est nécessaire;
- les priorités de traitement du risque en tenant compte des niveaux de risque appréciés.

*Il convient que les critères utilisés pour classer les risques par ordre de priorité tiennent compte des objectifs de l'organisme, des exigences contractuelles, légales et réglementaires, ainsi que de l'opinion des parties intéressées concernées. Le classement par ordre de priorité tel qu'il est effectué dans l'activité d'évaluation du risque est principalement basé sur les critères d'acceptation.*

## 1.7.5 Traitement du risque

### ISO/IEC 42001, article 6.1.3

*En tenant compte des résultats de l'appréciation du risque, l'organisme doit définir un processus de traitement des risques liés à l'IA pour:*

- a) sélectionner les options appropriées de traitement des risques liés à l'IA;
- b) déterminer toutes les mesures nécessaires pour mettre en œuvre les options de traitement du risque d'IA sélectionnées et comparer les mesures avec celles de l'Annexe A pour vérifier qu'aucune mesure requise n'a été omise;  
*NOTE 1 L'Annexe A fournit des mesures de référence pour atteindre les objectifs de l'organisme et traiter les risques liés à la conception et à l'utilisation des systèmes d'IA.*
- c) tenir compte des mesures de l'Annexe A qui sont pertinentes pour la mise en œuvre des options de traitement des risques liés à l'IA;
- d) identifier si des mesures supplémentaires sont nécessaires en plus de celles figurant à l'Annexe A afin de mettre en œuvre toutes les options de traitement du risque;
- e) tenir compte des orientations de l'Annexe B pour la mise en œuvre des mesures déterminées aux points b) et c)
- f) produire une déclaration d'applicabilité contenant les mesures requises et fournir les justifications de l'inclusion et de l'exclusion des mesures. La justification de l'exclusion peut inclure les cas où les mesures ne sont pas jugées nécessaires par l'appréciation du risque, et ceux où elles ne sont pas requises par les (ou sont soumises à des exceptions en vertu des) exigences externes applicables.
- g) formuler le plan de traitement des risques liés à l'IA.

**PECB**

123

### ISO/IEC42001, article6.1.3 Traitement des risques liés à l'IA (suite)

*NOTE2 Les objectifs des mesures sont implicitement inclus dans les mesures sélectionnées. L'organisme peut sélectionner un ensemble approprié d'objectifs de mesures et de mesures à partir de l'Annexe A. Les mesures énumérées dans l'Annexe A ne sont pas exhaustives et des objectifs de mesure et mesures additionnels peuvent être ajoutés si nécessaire. Si des mesures différentes ou supplémentaires sont nécessaires en plus de celles de l'Annexe A, l'organisme peut concevoir ces mesures ou les adopter à partir de sources existantes. Le management du risque lié à l'IA peut être intégré dans d'autres systèmes de management, le cas échéant.*

*NOTE3 L'organisme peut fournir des justifications documentées pour l'exclusion de tout objectif de mesure générique ou pour des systèmes d'IA spécifiques, qu'ils soient listés dans l'Annexe A ou établis par l'organisme lui-même.*

*L'organisme doit conserver des informations documentées sur le processus de traitement des risques lié à l'IA.*

# Traitement du risque

## ISO 31000, article 6.5.1

*Le traitement du risque a pour but de choisir et de mettre en œuvre des options pour aborder le risque.*

*Le traitement du risque implique un processus itératif:*

*formuler et choisir des options de traitement du risque;*

*s'il n'est pas acceptable, envisager un traitement complémentaire.*



*élaborer et mettre en œuvre le traitement du risque;*

*déterminer si le risque résiduel est acceptable;*

*apprécier l'efficacité de ce traitement;*

PECB

124

Il est préférable de concentrer initialement l'effort sur le traitement du risque de niveau supérieur, puis de procéder progressivement au traitement des risques de niveau inférieur.

Choisir la meilleure option de traitement du risque signifie que les coûts associés à la mise en œuvre de ces options n'excèdent pas les avantages qu'ils présentent. Les coûts devraient être au moins égaux aux avantages. Lors de la réalisation d'une telle analyse coûts-bénéfices, le contexte de l'organisation devrait également être pris en compte.

# Sélection des options de traitement du risque

## ISO 31000, article 6.5.2

*Les options de traitement du risque peuvent impliquer un ou plusieurs des éléments suivants:*

*un refus du risque marqué par la décision de ne pas commencer ou poursuivre l'activité porteuse du risque;*

*la prise ou l'augmentation d'un risque afin de saisir une opportunité;*

*l'élimination de la source de risque;*

*une modification de la vraisemblance;*

*une modification des conséquences;*

*un partage du risque (par exemple par le biais de contrats, de souscription de couvertures d'assurance);*

*un maintien du risque fondé sur une décision éclairée.*

PECB



125

## ISO23894, article 6.5.2 Sélection des options de traitement du risque

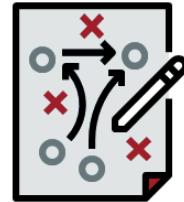
*Les recommandations données dans l'ISO31000:2018, 6.5.2, s'appliquent.*

*Il convient que les options de traitement du risque définies par l'organisme soient conçues pour réduire les conséquences négatives des risques à un niveau acceptable et pour accroître la vraisemblance de l'atteinte possible de conséquences positives. Si la réduction exigée des conséquences négatives ne peut pas être atteinte en appliquant différentes options de traitement du risque, il convient que l'organisme réalise une analyse bénéfice/risque des risques résiduels.*

# Élaboration et mise en œuvre des plans de traitement du risque

ISO/IEC 23894, article 6.5.3

- Les recommandations données dans l'ISO 31000:2018, 6.5.3, s'appliquent.
- Lorsque le plan de traitement du risque a été documenté, il convient que les mesures de traitement du risque sélectionnées en 6.5.2 soient mises en œuvre.
- Il convient que la mise en œuvre de chaque mesure de traitement du risque et son efficacité soient vérifiées et enregistrées conformément à 6.7.



PECB

126

## ISO31000, article6.5.3 Élaboration et mise en œuvre des plans de traitement du risque

Les plans de traitement du risque ont pour but de préciser la manière dont les options de traitement choisies seront mises en œuvre de sorte que les dispositions soient comprises par les personnes concernées et que les progrès par rapport au plan puissent faire l'objet d'un suivi.

Il convient que le plan de traitement identifie clairement l'ordre de mise en œuvre du traitement du risque.

Il convient que les plans de traitement soient intégrés aux plans et processus de management de l'organisme, en concertation avec les parties prenantes appropriées.

Il convient que les informations fournies dans le plan de traitement comportent:

- la justification du choix des options de traitement, y compris les avantages attendus;
- les personnes responsables de l'approbation et de la mise en œuvre du plan;
- les actions proposées;
- les ressources nécessaires, en tenant compte des impondérables;
- les mesures des performances;
- les contraintes;
- les rapports et le suivi requis;
- le moment où les actions sont censées être entreprises et achevées.

# Plan de traitement du risque

- Une fois que l'organisme a choisi l'option la plus pertinente de traitement du risque, il doit la planifier et la mettre en œuvre en conséquence.
- Les activités à entreprendre devraient être classées par ordre de priorité.
- L'organisme devrait allouer les ressources nécessaires à la mise en œuvre efficace de l'option de traitement du risque choisie.



PECB

127

Lorsqu'il détermine la priorité des actions à prendre pour mettre en œuvre l'option de traitement du risque choisie, il convient que l'organisme prenne en compte, entre autres, les éléments suivants:

- Les processus qui comportent le plus haut niveau de risque
- La nécessité de communiquer les résultats à la direction

# Exemple de plan de traitement du risque

Risque (vulnérabilité/menace) :	Insuffisance des processus de validation et de nettoyage des données pour les systèmes d'IA, entraînant l'utilisation de données de mauvaise qualité
Niveau de risque :	Six
Priorité :	Élevé
Option de traitement :	Modifier la vraisemblance et les conséquences
Détails de mesure :	Mettre en œuvre des protocoles rigoureux de validation et de nettoyage des données. Introduire des outils automatisés pour le contrôle de la qualité des données en temps réel et mettre en place un comité officiel de revue des données pour superviser les processus de traitement des données
Ressources nécessaires :	50 heures pour le développement et la mise en œuvre d'outils de validation des données
Responsable	David Smith, spécialiste des données et John McGee, responsable IA
Dates de début et de fin :	du 2024-05-01 au 2024-05-15
Maintenance nécessaire/commentaires :	Des appréciations régulières de la qualité des données et des ajustements des processus de validation seront essentiels. Un rapport sur la qualité des données devrait être produit après chaque réunion du comité

PECB

128

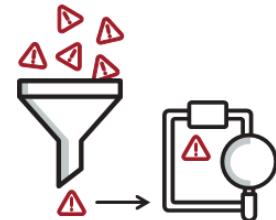
Tel que présenté sur la diapositive, le plan de traitement du risque adoptera probablement une approche plus ou moins élaborée, mais il devrait au moins clarifier les points suivants :

- Actions à prendre
- Ressources à allouer
- Responsabilités
- Priorités

# Évaluation des risques résiduels

ISO 31000, article 6.5.2

- Il convient que les décideurs et les autres parties prenantes soient informés de la nature et de l'étendue du risque résiduel après le traitement du risque.
- Il convient que le risque résiduel soit documenté et soumis à suivi et revue et, le cas échéant, fasse l'objet d'un traitement supplémentaire.



PECB

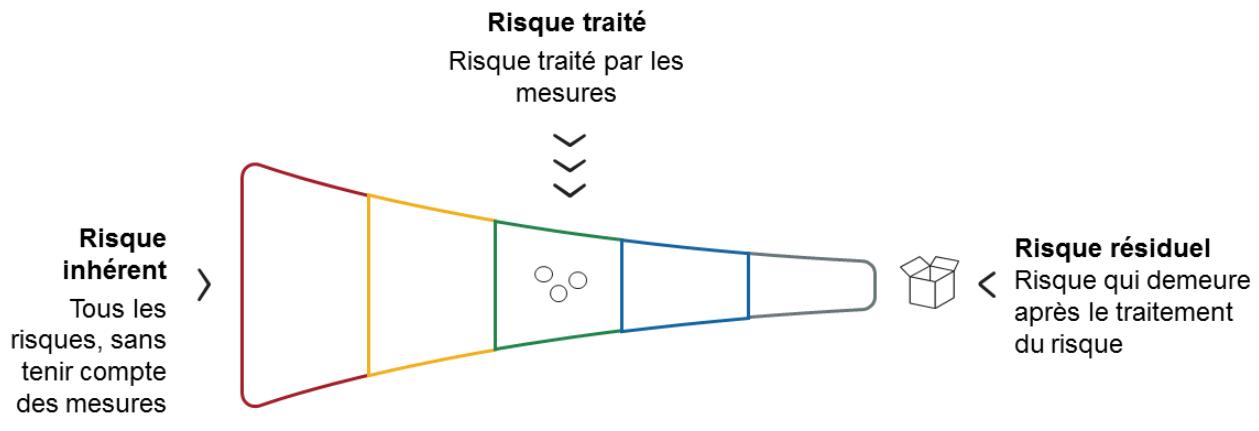
129

## ISO/IEC27005, article 8.6.3 Acceptation du risque résiduel en matière de sécurité de l'information

Afin de déterminer les risques résiduels, il convient que les plans de traitement du risque alimentent la réappréciation de la vraisemblance et des conséquences résiduelles. Il convient de tenir compte des moyens de maîtrise proposés dans les plans de traitement du risque et de leur efficacité pour déterminer s'ils réduiront la vraisemblance ou les conséquences, ou les deux, et si le niveau de risques résiduels est attribué aux risques. Le niveau de risques résiduels est ensuite examiné par le propriétaire du risque afin de déterminer si ces risques sont acceptables.

Il convient que les plans de traitement du risque décrivent la manière dont les risques vont être traités afin de remplir les critères d'acceptation des risques.

# Acceptation du risque résiduel



Les propriétaires de risque doivent être informés des risques résiduels et en accepter la responsabilité.

PECB

130

La notion de risque résiduel peut être définie comme étant le risque qui demeure après la mise en œuvre de mesures visant à réduire le risque inhérent et peut être résumée comme suit : **Risque résiduel = risque inhérent – risque traité**

Après la mise en œuvre d'un plan de traitement du risque, il y a toujours des risques résiduels. La valeur de la réduction des risques suivant le traitement des risques devrait être évaluée, calculée et documentée. Le risque résiduel peut être difficile à évaluer, mais une évaluation devrait être faite pour assurer que la valeur du risque résiduel respecte les critères d'acceptation du risque de l'organisme. L'organisme doit également mettre en place des mécanismes de surveillance des risques résiduels.

Si le risque résiduel est considéré comme inacceptable après la mise en œuvre des mesures, une décision doit être prise pour traiter entièrement le risque. Une option est d'identifier d'autres options de traitement des risques comme le partage des risques (assurance ou externalisation) pour réduire le risque à un niveau acceptable. Une autre option pourrait être d'accepter (volontairement) le risque. Même si c'est une bonne pratique de ne tolérer aucun risque pour lequel le critère d'acceptation des risques est défini par l'organisme, il n'est pas toujours possible de réduire tous les risques à un niveau acceptable. En toutes circonstances, les risques résiduels doivent être compris, acceptés et approuvés par la direction.

# Page de notes

---

PECB

131

## ***ISO/IEC27005, article8.6.3 Acceptation du risque résiduel en matière de sécurité de l'information***

*L'acceptation du risque peut impliquer un processus visant à obtenir l'approbation des traitements avant la décision finale d'acceptation du risque. Il est important que les propriétaires du risque revoient et approuvent les plans de traitement du risque proposés et les risques résiduels associés, puis enregistrent les conditions associées à l'approbation. En fonction du processus d'appréciation du risque et des critères d'acceptation du risque, il peut être nécessaire qu'un responsable ayant un niveau d'autorité supérieur à celui du propriétaire du risque valide l'acceptation du risque.*

*La mise en œuvre d'un plan permettant de traiter les risques appréciés peut prendre un certain temps. Les critères de risque peuvent permettre que les niveaux de risque dépassent un seuil souhaité dans une certaine mesure s'il existe un plan permettant de réduire ce risque dans un délai acceptable. Les décisions d'acceptation du risque peuvent tenir compte des délais prévus dans les plans de traitement du risque et du fait que la mise en œuvre du traitement du risque progresse ou non conformément à ce qui est prévu.*

*Certains risques peuvent varier dans le temps (que ce changement soit dû ou non à la mise en œuvre d'un plan de traitement du risque). Les critères d'acceptation du risque peuvent en tenir compte et avoir des seuils d'acceptation du risque qui dépendent de la durée pendant laquelle un organisme peut être exposé à un risque apprécié.*

## 1.7.6 Approbation du plan de traitement des risques IA

### ISO/IEC 42001, article 6.1.3

*L'organisme doit obtenir de la part des responsables désignés l'approbation du plan de traitement du risque et l'acceptation des risques résiduels liés à l'IA. Les mesures nécessaires doivent:*

- être alignées sur les objectifs en 6.2;
- être disponibles sous forme d'information documentée;
- être communiquées au sein de l'organisme;
- être mise à la disposition des parties intéressées, le cas échéant.

*L'organisme doit conserver des informations documentées sur le processus de traitement des risques liés à l'IA.*

## 1.7.7 Communication et consultation

ISO 31000, article 6.2

*La communication et la consultation ont pour but d'aider les parties prenantes pertinentes à comprendre le risque, les principes de prise de décisions et les raisons pour lesquelles certaines actions sont nécessaires.*



PECB

133

### **ISO/IEC 23894, article 6.2 Communication et consultation (suite)**

*Les recommandations données dans l'ISO31000:2018, 6.2, s'appliquent.*

*L'ensemble de parties prenantes pouvant être affectées par des systèmes d'IA peut être plus vaste que celui initialement prévu et peut inclure des parties prenantes externes qui ne seraient pas considérées dans un cas contraire et s'étendre à d'autres parties d'une société.*

Une bonne communication et une bonne consultation exigent des réunions régulières avec toutes les parties intéressées afin que tous leurs besoins et attentes soient identifiés et satisfaits.

Pour obtenir des résultats bénéfiques, il est important d'élaborer avant tout une stratégie de communication, puis de la mettre en œuvre.

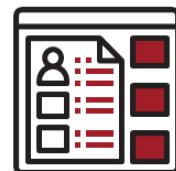
La deuxième partie importante est la consultation. Le gestionnaire de risques est considéré comme un consultant interne ou un encadreur qui aide les salariés moins expérimentés à acquérir l'expertise nécessaire en matière de management des risques afin d'atteindre les objectifs d'optimisation des risques.

## 1.7.8 Enregistrement et élaboration de rapports

### ISO 31000, article 6.7

*Il convient que le processus de management du risque et ses résultats soient documentés et fassent l'objet de rapports selon des mécanismes appropriés. L'enregistrement et l'élaboration de rapports a pour but de:*

- communiquer sur les activités de management du risque et leurs résultats au sein de l'organisme;
- fournir des informations en vue de la prise de décisions;
- améliorer les activités de management du risque;
- faciliter l'interaction avec les parties prenantes, y compris celles ayant la responsabilité des activités de management du risque.



*Il convient que les décisions concernant la création, la conservation et le traitement des informations documentées tiennent compte, sans toutefois s'y limiter, de leur utilisation, du caractère sensible des informations et du contexte externe et interne.*

PECB

134

### ISO/IEC 23894, article 6.7 Enregistrement et élaboration de rapports

*Les recommandations données dans l'ISO31000:2018, 6.7, s'appliquent.*

*Il convient que l'organisme établisse, enregistre et tienne à jour un système pour la collecte et la vérification des informations sur le produit ou des produits similaires, dès les phases de mise en œuvre et qui font suite à la mise en œuvre. Il convient également que l'organisme collecte et passe en revue les informations publiquement disponibles sur des systèmes similaires disponibles sur le marché.*

*Il convient que ces informations soient ensuite appréciées pour déterminer leur pertinence possible pour la fiabilité du système d'IA. En particulier, il convient que l'évaluation apprécie si des risques précédemment non détectés existent ou si des risques précédemment appréciés ne sont plus acceptables. Ces informations peuvent être utilisées et factorisées au sein du processus de management du risque lié à l'IA de l'organisme, en tant qu'ajustement des objectifs, des cas d'utilisation ou des enseignements tirés.*

*Si l'une de ces conditions s'applique, il convient que les organismes réalisent les activités suivantes:*

- apprécier l'impact des activités précédentes de management du risque et ajouter des résultats de cette appréciation au processus de management du risque;
- passer en revue les activités de management du risque pour le système d'IA. S'il est possible que le risque résiduel ou que son acceptation ait été modifiée(e), il convient que les effets sur les mesures existantes de maîtrise du risque soient évalués.

*Il convient que les résultats de cette appréciation soient enregistrés. Il convient que l'enregistrement du management du risque permette la traçabilité de chaque risque identifié dans l'ensemble des processus de management du risque. Les enregistrements peuvent s'appuyer sur un modèle commun approuvé par l'organisme.*

# Page de notes

---

PECB

135

## ***ISO/IEC 23894, article 6.7 Enregistrement et élaboration de rapports (suite)***

*Outre la documentation du périmètre d'application, du contexte et des critères, l'appréciation du risque et le traitement du risque, il convient que l'enregistrement inclut au moins les informations suivantes:*

- *description et identification du système analysé;*
- *méthodologie appliquée;*
- *description de l'utilisation prévue du système d'IA;*
- *identité de la ou des personnes et de l'organisme qui ont réalisé l'appréciation du risque;*
- *référence et date de l'appréciation du risque;*
- *conclusions de l'appréciation du risque;*
- *si et dans quelle mesure les objectifs ont été satisfait.*

## 1.7.9 Suivi et revue

ISO 31000, article 6.6

- *Le suivi et la revue ont pour but de s'assurer et d'améliorer la qualité et l'efficacité de la conception, de la mise en œuvre et des résultats du processus.*
- *Il convient que le suivi continu et la revue périodique du processus de management du risque et de ses résultats soient planifiés dans le processus de management du risque, en définissant clairement les responsabilités.*



PECB

136

### **ISO31000, article6.6 Suivi et revue (suite)**

*Il convient que le suivi et la revue aient lieu à toutes les étapes du processus. Le suivi et la revue comprennent la planification, le recueil et l'analyse d'informations, l'enregistrement des résultats et le retour d'information.*

*Il convient d'intégrer les résultats du suivi et de la revue aux activités de management des performances de l'organisme, de suivi des résultats et d'élaboration de rapports.*

### **ISO/IEC23894, article6.6 Suivi et revue**

*Les recommandations données dans l'ISO31000:2018, 6.6, s'appliquent.*

Un mesurage continu des performances fournit des informations précieuses sur le moment et l'endroit où l'attention doit être portée pour améliorer le système. Avoir une meilleure vue d'ensemble (grâce aux informations de mesurage) du paysage des risques permet aux organismes de préparer et de mettre en œuvre de meilleures stratégies qui tiennent compte des opportunités et des écueils constatés. Par ailleurs, les programmes de surveillance permettent de fournir les informations nécessaires sur les risques significatifs et les tendances de risques émergents, ainsi que sur leur impact sur les objectifs et la stratégie globale de l'organisme. [1]

# Résumé de la section :

- Le management des risques liés à l'IA devrait être intégré, structuré, complet, personnalisé, inclusif, dynamique, s'appuyer sur les meilleures informations disponibles, tenir compte des facteurs humains et culturels et faire l'objet d'amélioration continue.
- Pour un management efficace des risques liés à l'IA dans les organismes, il est essentiel d'élargir le périmètre, de contextualiser le processus et d'établir des critères pour évaluer l'importance des risques liés au développement et à l'utilisation de l'IA, l'inventaire qui en découle étant documenté comme partie intégrante de la procédure globale de management des risques.
- L'organisme doit identifier les risques, indépendamment du contrôle exercé sur leurs sources, en tenant compte des divers résultats potentiels et des conséquences associées.
- L'analyse du risque devrait englober des facteurs tels que la vraisemblance d'un incident, la nature et l'ampleur des conséquences, la complexité, la connectivité, les aspects temporels, la volatilité, l'efficacité des mesures existantes, la sensibilité et les niveaux de confiance.
- La finalité de l'évaluation du risque est l'aide à la décision, qui implique de comparer les résultats de l'analyse du risque avec les critères de risque prédéfinis afin d'identifier les domaines nécessitant une action spécifique.
- L'objectif du traitement du risque est de sélectionner et d'exécuter des mesures pour gérer les risques.

PECB



Questions ?



Exercice 2



Quiz 11

137

**Note:**Pour répondre à l'Exercice2 et au Quizz11, veuillez accéder à la fiche des Exercices et à la fiche des Quizz , respectivement.

# Section 13

## Déclaration d'applicabilité

- Rédaction de la Déclaration d'applicabilité
- Approbation de la direction
- Revue et sélection des mesures d'IA applicables
- Justification des mesures de sécurité sélectionnées
- Justification des mesures de sécurité exclues

PECB

138

Cette section fournit des informations qui aideront le participant à identifier les mesures d'IA à inclure dans le SMIA, à justifier le choix des mesures sélectionnées et exclues, et à obtenir l'approbation formelle de la direction pour la mise en œuvre du système de management de l'IA.

# Déclaration d'applicabilité

1. Définir et établir		2. Mettre en œuvre et opérer		3. Surveiller et revoir		4. Maintenir et améliorer	
1.1	Leadership et approbation du projet	2.1	Sélection et conception des mesures	3.1	Surveillance, mesurage, analyse et évaluation	4.1	Traitemet des non-conformités
1.2	Rôles et responsabilités	2.2	Mise en œuvre des mesures	3.2	Audit interne	4.2	Amélioration continue
1.3	L'organisme et son contexte	2.3	Gestion des informations documentées	3.3	Revue de direction		
1.4	Périmètre du SMIA	2.4	Communication				
1.5	Analyse du système existant	2.5	Compétence et sensibilisation				
1.6	Politique d'IA	2.6	Gestion des opérations d'IA				
1.7	Management du risque lié à l'IA						
1.8	<b>Déclaration d'applicabilité</b>						

PECB

139

# ISO/IEC 42001 Exigences concernant la Déclaration d'applicabilité.

## ISO/IEC 42001, article 6.1.3

*En tenant compte des résultats de l'appréciation du risque, l'organisme doit définir un processus de traitement des risques liés à l'IA pour:*

- f) produire une déclaration d'applicabilité contenant les mesures requises [voir b), c) et d)] et la justification de leur inclusion et exclusion. La justification de l'exclusion peut inclure les cas où les mesures ne sont pas jugées nécessaires par l'appréciation du risque, et ceux où elles ne sont pas requises par les (ou sont soumises à des exceptions en vertu des) exigences externes applicables.

**Note :** La norme ISO/IEC 42001 n'exige pas que les organismes sélectionnent seulement des mesures listées dans l'Annexe A. Ils peuvent également sélectionner des mesures à partir d'autres sources ou les concevoir eux-mêmes.

PECB

140

### **ISO/IEC42001, article6.1.3 Traitement des risques liés à l'IA (suite)**

*NOTE3 L'organisme peut fournir des justifications documentées pour l'exclusion de tout objectif de mesure générique ou pour des systèmes d'IA spécifiques, qu'ils soient listés dans l'Annexe A ou établis par l'organisme lui-même.*

# Déclaration d'applicabilité

- Une déclaration d'applicabilité (DdA) est une déclaration documentée énumérant les mesures qui sont pertinentes et applicables au SMIA de l'organisme.
- La DdA contient les justifications de l'organisme pour l'inclusion de certaines mesures de l'Annexe A, ainsi que les justifications pour l'exclusion d'autres mesures.
- La déclaration d'applicabilité représente davantage qu'une liste de contrôle des mesures d'IA de l'Annexe A de l'ISO/IEC 42001 à mettre en œuvre dans le SMIA de l'organisme. C'est un document clé du SMIA qui sert de référence pour l'auditeur externe durant l'audit de certification ; en tant que tel, c'est l'une des premières informations documentées qui fera l'objet d'une analyse. C'est également l'une des informations documentées que la direction de l'organisme doit valider et approuver avant de lancer les opérations du SMIA.

PECB

141

## ***ISO/IEC42001, article3.26 Déclaration d'applicabilité***

*Documentation de toutes les mesures nécessaires et justification de l'inclusion ou de l'exclusion des mesures*

*Note1 à l'article: Les organismes peuvent ne pas nécessiter toutes les mesures énumérées en Annexe A ou peuvent même nécessiter des mesures additionnelles établies par l'organisme lui-même.*

*Note2 à l'article: Tous les risques identifiés doivent être documentés par l'organisme conformément aux exigences du présent document. Tous les risques identifiés et les mesures de gestion des risques établies pour les traiter doivent être représentés dans la déclaration d'applicabilité.*

# Déclaration d'applicabilité

- La norme ISO/IEC 42001 ne fournit pas d'explications détaillées sur la manière dont la déclaration d'applicabilité doit être élaborée. Elle mentionne seulement brièvement qu'elle doit contenir une liste des mesures d'IA ainsi que la justification de leur inclusion et de leur exclusion, le cas échéant, par rapport aux mesures de l'Annexe A.
- Les organismes peuvent inclure les éléments suivants dans la DdA :
  - ▷ Mesure d'IA
  - ▷ Applicabilité
  - ▷ Description sommaire
  - ▷ Justification
  - ▷ Informations documentées
  - ▷ Responsabilité

PECB

142

- **Mesure d'IA:** Cette section indique les mesures de l'Annexe A d'ISO/IEC42001 ou de toute autre source identifiée par l'organisme.
- **Applicabilité :** Dans cette section, on indique si la mesure s'applique ou non à l'organisme. Une mesure est considérée comme applicable si sa mise en œuvre permet de traiter les risques identifiés, si elle est requise par la loi, s'il s'agit d'une exigence contractuelle, etc. L'applicabilité des mesures dépend de l'organisme, de la nature et de la gravité des risques, ainsi que du périmètre du SMIA.
- **Description sommaire :** Cette section fournit une description de la mesure et indique comment elle est prévue d'être mise en œuvre dans l'organisme. Une façon simple de procéder consiste à utiliser la méthode des «6W» (qui, quoi, quand, où, pourquoi, comment), à l'exception du «pourquoi» qui doit être abordé dans la section «justification».
- **Justification:** Dans cette section sont fournies les raisons du choix ou de l'exclusion d'une mesure d'IA.
- **Informations documentées :** Dans cette section figurent les documents (politiques et procédures) relatifs aux mesures d'IA.
- **Responsabilité :** Cette section contient le nom et la fonction de la personne responsable de la mesure.

# 1.8 Déclaration d'applicabilité

## Liste des activités

1.8.1

Revoir et sélectionner les mesures  
d'IA applicables

1.8.3

Justifier les mesures exclues

1.8.2

Justifier les mesures sélectionnées

1.8.4

Finaliser la déclaration d'applicabilité

PECB

143

## 1.8.1 Revoir et sélectionner les mesures d'IA applicables

- L'organisme doit examiner les mesures d'IA de l'Annexe A afin d'identifier celles qui sont applicables et celles qui ne le sont pas dans son contexte.
- Le choix d'appliquer ou non une mesure d'IA devrait se justifier essentiellement par l'appréciation du risque. C'est pourquoi la déclaration d'applicabilité ne devrait pas être rédigée avant le dépôt du rapport d'analyse du risque et de traitement du risque.



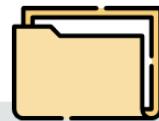
PECB

144

Les mesures d'IA proposées dans l'Annexe A peuvent se révéler suffisantes pour traiter l'ensemble des scénarios de risque que l'organisme a identifiés. D'autres référentiels peuvent être utilisés et intégrés dans le SMIA pour mettre en œuvre des mesures d'IA supplémentaires. Il convient de noter que les mesures supplémentaires doivent également être décrites dans la Déclaration d'applicabilité.

## 1.8.2 Justifier les mesures sélectionnées

- Il convient que l'organisme justifie le choix de chaque mesure incluse dans le SMIA.
- C'est la réponse au « Pourquoi ? » de chaque mesure.



### Processus d'évaluation de l'impact du système d'IA (ISO/IEC 42001, Annexe A.5.2) :

*L'organisme doit définir un processus d'évaluation des conséquences potentielles, pour les personnes ou les groupes de personnes, ou les deux, ainsi que pour les sociétés, de la mise en œuvre d'un système d'IA tout au long de son cycle de vie.*

**Justification de la sélection :** Cette mesure est choisie pour identifier et atténuer de manière proactive toute conséquence négative découlant du système d'IA, en assurant une approche globale visant à minimiser les dommages causés aux personnes et à la société.

PECB

145

Voici quelques exemples de justifications liées à des mesures sélectionnées:

### ISO/IEC42001, AnnexeA.6.2.5 Déploiement d'un système d'IA

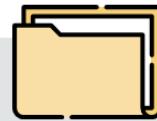
*L'organisme doit documenter un plan de déploiement et s'assurer que les exigences appropriées sont satisfaites avant le déploiement.*

**Justification de la sélection :** Cette mesure est choisie pour assurer un processus de déploiement sûr et contrôlé, garantissant ainsi le fonctionnement efficace du système d'IA tout en satisfaisant à tous les critères nécessaires en matière de fonctionnalité, de sécurité et de conformité.

## 1.8.3 Justifier les mesures exclues

Il convient que l'organisme justifie l'exclusion de chaque mesure d'IA présentée dans l'Annexe A de la norme ISO/IEC 42001.

**Exemple :**



***ISO/IEC 42001, Annexe A.3.3 Signalement des préoccupations***

*L'organisme doit définir et mettre en place un processus permettant de signaler les préoccupations concernant le rôle de l'organisme à l'égard d'un système d'IA tout au long de son cycle de vie.*

**Justification de l'exclusion :** Conformément aux protocoles et structures organisationnels existants pour la résolution des problèmes, l'organisme dispose déjà de canaux bien établis permettant aux employés de faire part de leurs préoccupations concernant tout aspect de ses activités, y compris celles liées aux systèmes d'IA.

## 1.8.4 Finaliser la Déclaration d'applicabilité

### Exemple

Mesure	Applicable	Description	Justification	Documentation	Responsable
ISO/IEC 42001, Annexe A 5.2 <i>Processus d'évaluation de l'impact du système d'IA</i>	Oui	L'organisme a mis en place un processus d'évaluation de l'impact de l'IA qui évalue les effets des systèmes d'IA sur les personnes et la société. Ce processus est intégré dans le cycle de développement des systèmes d'IA.	S'assurer que les systèmes d'IA sont développés et mis en œuvre de manière responsable, en évaluant les conséquences potentielles sur les personnes et la société.	AI-Impact-Assessment-Procedure-4202AP	Comité d'éthique de l'IA

PECB

147

# Finaliser la Déclaration d'applicabilité (suite)

## Exemple

Mesure	Applicable	Description	Justification	Documentation	Responsable
ISO/IEC 42001, Annexe A 3.3 <i>Signalement des préoccupations</i>	Non	-----	Conformément aux protocoles organisationnels existants, les canaux actuels de résolution des problèmes couvrent suffisamment le signalement des préoccupations liées aux systèmes d'IA, ce qui rend inutile un processus distinct.	N/A	N/A

PECB

148

## 1.8.5 Obtenir l'approbation de la direction

---

- Une collaboration étendue, du temps, des efforts et un engagement fort de la part de la direction sont essentiels pour la planification de la DdA au niveau de l'entreprise.
- La DdA devrait constituer un tableau de contrôle concis et soumis à l'examen et à l'approbation de la direction.



# Résumé de la section :

- Une déclaration d'applicabilité (DdA) est une déclaration documentée énumérant les mesures qui sont pertinentes et applicables au SMIA de l'organisme. La DdA contient non seulement les justifications de l'organisme d'inclure certaines mesures de l'Annexe A, mais également les justifications d'exclure d'autres mesures.
- L'organisme doit examiner les mesures d'IA de l'Annexe A afin d'identifier celles qui sont applicables et celles qui ne le sont pas dans son contexte.
- Le choix d'appliquer ou non une mesure d'IA devrait se justifier essentiellement par l'appréciation du risque. C'est pourquoi la déclaration d'applicabilité ne devrait pas être rédigée avant le dépôt du rapport d'analyse du risque et de traitement du risque.



Questions ?

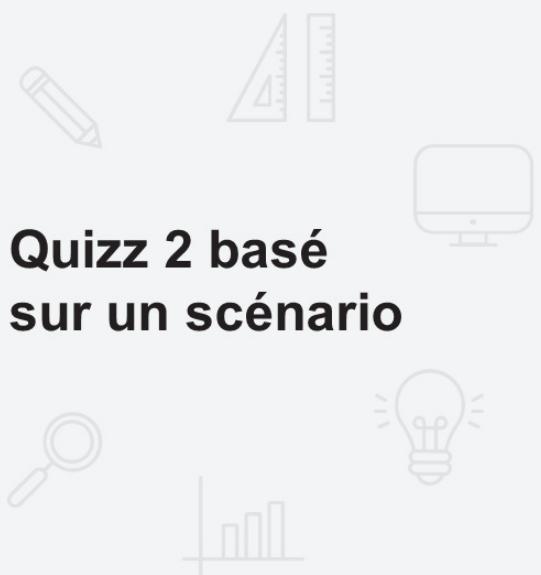


Quizz 12

PECB

150

**Note:**Pour répondre au Quizz12, veuillez accéder à la fiche Quizz.



## Quizz 2 basé sur un scénario

PECB



151

**Note:**Pour répondre au Quizz2 basé sur un scénario, veuillez accéder à la fiche Quizz.

# Résumé du Jour 2

Les sujets suivants ont été abordés lors de cette journée de formation :

- Contexte de l'organisme
- Périmètre du SMIA
- Analyse du système existant
- Politique d'IA
- Politiques d'IA spécifiques
- Appréciation du risque
- Traitement du risque
- Acceptation du risque
- Déclaration d'applicabilité
- Justification des mesures d'IA sélectionnées
- Justification des mesures d'IA exclues