Commented [AES1]: Pour apprendre à remplir ce document et pour consulter des exemples concrets de ce que vous devez rédiger, regardez ce tutoriel vidéo "How to Write the ISO 27001 Risk Assessment Methodology".

Pour accéder au tutoriel : dans votre boîte de réception, consultez l'e-mail que vous avez reçu au moment de l'achat. Vous y trouverez un lien et un mot de passe qui vous permettront d'accéder au tutoriel vidéo.

[Logo de l'organisation]

[Nom de l'organisation]

Commented [AES2]: Remplissez tous les champs entre crochets [ ] dans ce document.

METHODOLOGIE D'EVALUATION ET DE TRAITEMENT DES RISQUES

Commented [AES3]: Pour apprendre à rédiger la méthodologie, consultez ces articles :

- ISO 27001 risk assessment & treatment – six main steps https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/#section2
- How to write ISO 27001 risk assessment methodology https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/#section3

Code :	
Version :	
Date de la version :	
Créé par :	
Approuvée par :	
Niveau de confidentialité :	

Commented [AES4]: Le système de codage des documents doit être aligné avec le système existant de l'organisation pour la codification des documents ; au cas où un tel système n'est pas en place, cette ligne peut être supprimée.

Historique des modifications

Date	Version	Créé par	Description de la modification
	0.1	Advisera	Structure documentaire de base

Table des matières

1. But, domaine d'application et utilisateurs

Ce document a pour but de définir la méthodologie pour l'évaluation et le traitement des risques de l'information au sein de [nom de l'organisation], et de définir le niveau acceptable de risque, conformément à la norme ISO/IEC 27001.

L'évaluation et le traitement des risques sont appliqués à l'ensemble du domaine d'application du Système de management de la sécurité de l'information (SMSI), c'est-à-dire à tous les actifs utilisés au sein de l'organisation ou qui peuvent avoir un impact sur la sécurité de l'information au sein du SMSI.

Les utilisateurs de ce document sont tous les employés de [nom de l'organisation] qui prennent part à l'évaluation et au traitement des risques.

2. Documents référencés

- Norme ISO/IEC 27001, clauses 6.1.2, 6.1.3, 8.2 et 8.3
- Norme ISO 22301, clauses 8.2.1 et 8.2.3
- Politique de sécurité de l'information
- Liste des exigences légales, réglementaires, contractuelles et autres
- Politique de sécurité des fournisseurs
- Déclaration d'applicabilité

3. Méthodologie d'évaluation et de traitement des risques

3.1. Evaluation des risques

3.1.1. Le processus

L'évaluation des risques est mise en œuvre au travers du Tableau d'évaluation des risques. Le processus d'évaluation des risques est coordonné par [titre du poste], l'identification des menaces et des vulnérabilités est réalisée par les propriétaires des actifs et l'évaluation des impacts et vraisemblances est menée par les propriétaires des risques. [illegible]

3.1.2. Actifs, vulnérabilités et menaces

La première étape dans l'évaluation des risques consiste à identifier tous les actifs dans le domaine d'application du SMSI, tâche réalisée par les représentants de chaque secteur dans le domaine d'application du SMSI - c'est-à-dire identifier tous les actifs pouvant affecter la confidentialité, [illegible]

Commented [AES5]: Indiquez le nom de votre organisation.

Commented [AES6]: Ou ISO 22301

Commented [AES7]: Ou "Système de management de la continuité des activités (SMCA)"

Commented [AES8]: Ou SMCA

Commented [AES9]: Indiquez le nom de votre organisation.

Commented [AES10]: Effacer ceci si vous ne mettez pas en œuvre la sécurité de l'information.

Commented [AES11]: Effacer ceci si vous ne mettez pas en œuvre la continuité des activités.

Commented [AES12]: Effacer ceci si vous ne mettez pas en œuvre la sécurité de l'information.

Commented [AES13]: Effacez si vous n'utilisez pas cette Politique.

Commented [AES14]: Effacer ceci si vous ne mettez pas en œuvre la sécurité de l'information.

Commented [AES15]: Cette méthodologie doit être modifiée si [illegible]

Commented [AES16]: Pour simplifier le processus, vous pouvez indiquer que le propriétaire des actifs pour chaque risque est également le propriétaire du risque.

[illegible]

Commented [AES17]: Ou SMCA

Commented [AES18]: Ou SMCA

personnes, des équipements informatiques, l'infrastructure et des services / processus automatisés. Lors de l'identification des actifs, il est assez nécessaire d'identifier leurs propriétaires - les personnes ou entités organisationnelles responsables pour chaque actif.

Commented [AES19]: Ajouter également d'autres types d'actifs

L'étape suivante consiste, pour les propriétaires des actifs, à identifier toutes les menaces et vulnérabilités associées à chacun des actifs. Les menaces et les vulnérabilités sont identifiées à l'aide des répertoires inclus dans le Tableau d'évaluation des risques. Chaque actif peut être associé à plusieurs menaces et chaque menace peut être associée à plusieurs vulnérabilités.

3.1.3. Détermination des propriétaires des risques

Pour chaque risque, un propriétaire du risque doit être identifié - la personne ou l'unité organisationnelle responsable de chaque risque. Cette personne n'est pas nécessairement le propriétaire de l'actif.

Commented [AES20]: Pour simplifier le processus, vous pouvez

3.1.4. Impacts et vraisemblances

Une fois les propriétaires des risques identifiés, il est nécessaire d'évaluer l'impact pour chaque combinaison de menaces et vulnérabilités, d'un actif donné, si un tel risque se réalise :

Impact faible	0	Perte de confidentialité, de disponibilité ou d'intégrité n'affectant pas le flux de trésorerie de l'organisation, ses obligations légales ou contractuelles, ou sa réputation.
Impact modéré	1	Perte de confidentialité, de disponibilité ou d'intégrité entraînant des coûts et ayant un impact faible ou modéré sur les obligations légales ou contractuelles, ou sur la réputation de l'organisation.
Impact élevé	2	Perte de confidentialité, de disponibilité ou d'intégrité ayant un impact considérable et / ou immédiat sur le flux de trésorerie de l'organisation, sur ses opérations, sur ses obligations légales ou contractuelles, ou sur sa réputation.

Après l'évaluation de l'impact, il est nécessaire d'évaluer la probabilité qu'un tel risque se réalise, c'est-à-dire la probabilité qu'une menace exploite la vulnérabilité de l'actif concerné :

Faible vraisemblance	0	Les mesures de sécurité existantes sont importantes et ont, jusqu'à présent, fourni un niveau de protection adéquat. Aucun nouvel incident n'est attendu à l'avenir.
Vraisemblance modérée	1	Les mesures de sécurité existantes sont modérées et ont généralement fourni un niveau de protection adéquat. De nouveaux incidents sont possibles mais il est peu probable.
Vraisemblance élevée	2	Les mesures de sécurité existantes sont faibles ou inefficaces. De tels incidents ont une probabilité élevée de se produire à l'avenir.

En indiquant les valeurs d'impact et de vraisemblance dans le Tableau d'évaluation des risques, le niveau de risque est calculé automatiquement par l'addition des deux valeurs. [illegible]

3.2. Critères d'acceptation des risques

Les risques de niveaux 0, 1 et 2 sont des risques acceptables, alors que les risques de niveaux 3 et 4 sont des risques inacceptables. Les risques inacceptables doivent être traités.

3.3. Traitement des risques

Le traitement des risques est mis en œuvre au travers du Tableau de traitement des risques, en copiant tous les risques identifiés comme inacceptables depuis le Tableau d'évaluation des risques. [illegible]

Commented [AES21]: Par ex. Responsable continuité d'activité, [illegible]

Une ou plusieurs options de traitement doivent être sélectionnées pour les risques de niveaux 3 et 4 :

1. Sélection des mesures de sécurité ou des mesures à partir de [indiquer ici la source des mesures à utiliser].
2. Transfert des risques à un tiers – par exemple en souscrivant une police d'assurance ou en signant un contrat avec des fournisseurs ou des partenaires.
3. [illegible]
4. [illegible]

Commented [AES22]: Par ex. mesures de l'Annexe A de la norme ISO 27001, publication spéciale du NIST, etc.

[illegible]

Commented [AES23]: La sélection des mesures de sécurité doit prendre en compte les options qui :
- protègent les activités commerciales et réduisent la probabilité d'une perturbation
- [illegible]

La sélection des options est mise œuvre au travers du Tableau de traitement des risques. L'option 1 est généralement sélectionnée : la sélection d'une ou de plusieurs mesures de sécurité. Lorsque plusieurs mesures de sécurité sont sélectionnées pour un risque, des lignes supplémentaires sont insérées dans le tableau juste en-dessous de la ligne définissant le risque.

[illegible]

Commented [AES24]: Effacez si vous n'utilisez pas cette Politique.

[illegible]

Commented [AES25]: Cette nouvelle valeur est appelée "Risque résiduel".

3.4. Révisions régulières de l'évaluation et du traitement des risques

Les propriétaires des risques doivent procéder à un examen des risques existants et mettre à jour le Tableau d'évaluation des risques et le Tableau de traitement des risques en fonction des risques nouvellement identifiés. [illegible]

3.5. Déclaration d'applicabilité et Plan de traitement des risques

[Titre du poste] doit consigner les éléments suivants dans la Déclaration d'applicabilité : les mesures de sécurité de l'Annexe A de la norme ISO/IEC 27001 applicables et celles qui ne le sont pas, les justifications de telles décisions et si elles sont ou non effectivement implémentées.

[illegible]

[illegible]

3.6. Rapports

[Titre du poste] consignera les résultats de l'évaluation et du traitement des risques, et de toutes les révisions ultérieures, dans le Rapport d'évaluation et de traitement des risques.

[illegible]

4. Gestion des enregistrements conservés sur la base de ce document

Nom de l'enregistrement	*Lieu de conservation*	[illegible]	[illegible]	[illegible]
Tableau d'évaluation des risques (forme électronique - document Excel)	Ordinateur de [titre du poste]	[illegible]	[illegible]	[illegible]
Tableau de traitement des risques (forme électronique - document Excel)	Ordinateur de [titre du poste]	[illegible]	[illegible]	[illegible]
Rapport d'évaluation et de traitement des risques (forme électronique -	Ordinateur de [titre du poste]	[illegible]	[illegible]	[illegible]

Commented [AES26]: Effacer ceci si vous ne mettez pas en

Commented [AES27]: Si, pour une raison quelconque, l'acceptation du risque ne fait pas partie de la Déclaration d'applicabilité (par ex. de trop nombreuses personnes peuvent avoir accès à la Déclaration),

Commented [AES28]: Vous pouvez consulter un modèle pour

Commented [AES29]: Par ex. Responsable continuité d'activité,

Commented [AES30]: Par ex. Responsable continuité d'activité,

Commented [AES31]: Il ne s'agit que d'une recommandation.

Commented [AES32]: Par ex. PDG, responsable de l'unité opérationnelle, etc.

Commented [AES33]: Dans cette colonne, indiquez les données

Commented [AES34]: Par ex. Responsable continuité d'activité,

Commented [AES35]: Par ex. Responsable continuité d'activité,

format PDF)				
Déclaration d'applicabilité (forme électronique - format PDF)	Ordinateur de [titre du poste]	[titre du poste du propriétaire du Rapport]	[seul [titre du poste] est autorisé à saisir des données dans la Déclaration d'applicabilité et à la modifier]	[les archives version de la DdA sont conservées pendant une durée de 3 ans]
Plan de traitement des risques (forme électronique - document Word	Ordinateur de [titre du poste]	[titre du poste de la personne responsable du Plan de traitement des risques]	[seul [titre du poste] est autorisé à saisir des données dans le Plan de traitement des risques et à le modifier]	[les archives versions du Plan de traitement des risques sont conservées pendant une durée de 3 ans]

Seul [titre du poste] peut accorder à d'autres employés l'accès aux documents mentionnés ci-dessus.

Commented [AES36]: Effacer ceci si vous ne mettez pas en [illegible]

Commented [AES37]: Par ex. Responsable continuité d'activité, [illegible]

5. Validité et gestion documentaire

Ce document est valide à compter du [date].

Le propriétaire de ce document est [titre du poste], qui doit vérifier et, si nécessaire, mettre à jour ce document au moins [une fois par an], avant l'examen régulier de l'évaluation des risques entrants.

Commented [AES38]: Par ex. Responsable continuité d'activité, [illegible]

Commented [AES39]: Il ne s'agit que d'une recommandation ; [illegible]

Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être considérés :

- le nombre d'incidents qui se sont produits mais qui n'ont pas été inclus dans l'évaluation des risques
- le nombre de risques qui n'ont pas été traités correctement
- le nombre d'erreurs dans le processus d'évaluation et de traitement des risques en raison de la définition imprécise des fonctions et des responsabilités

6. Annexes

- Annexe 1 – Tableau d'évaluation des risques
- Annexe 2 – Tableau de traitement des risques
- Annexe 3 – Rapport d'évaluation et de traitement des risques

[titre du poste]
[nom]

[signature]

Commented [AES40]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.