Annexe 3 – Rapport d'évaluation et de traitement des risques

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 ISO 27001 Risk Assessment Report".

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.

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 2
2. DOCUMENTS REFERENCES 2
3. PROCESSUS D'EVALUATION ET DE TRAITEMENT DES RISQUES DE L'INFORMATION 2
   - 3.1. BUT DE LA GESTION DES RISQUES 2
   - 3.2. DOMAINE D'APPLICATION DE L'EVALUATION ET DU TRAITEMENT DES RISQUES 2
   - 3.3. DUREE 2
   - 3.4. PARTICIPANTS AU PROCESSUS ET COLLECTE DE L'INFORMATION 3
   - 3.5. BREF APERÇU DE LA METHODOLOGIE APPLIQUEE 3
   - 3.6. APERÇU DES DOCUMENTS UTILISES PENDANT LE PROCESSUS D'EVALUATION ET DE TRAITEMENT DES RISQUES 3
4. VALIDITE ET GESTION DOCUMENTAIRE 4
5. ANNEXES 4

1. But, domaine d'application et utilisateurs

Ce document a pour but de présenter un aperçu détaillé du processus et des documents utilisés au cours de l'évaluation et du traitement des risques de l'information au sein de [nom de l'organisation] pendant la période [préciser la période].

L'évaluation des risques a été appliquée à l'ensemble du Système de management de la sécurité de l'information (SMSI).

Ce document est destiné à la direction de [nom de l'organisation], au [titre du poste responsable de la sécurité de l'information], aux propriétaires d'actifs informationnels et à toutes personnes impliquées dans la planification, la mise en œuvre, le suivi et l'amélioration du SMSI.

2. Documents référencés

- Norme ISO/IEC 27001, clauses 8.2 et 8.3
- Norme ISO 22301, clause 8.2.3
- Document du domaine d'application du SMSI
- Politique de sécurité de l'Information
- Politique de continuité des activités
- Méthodologie d'évaluation et de traitement des risques

3. Processus d'évaluation et de traitement des risques de l'information

L'ensemble du processus d'évaluation et de traitement des risques a été réalisé conformément au document de Méthodologie d'évaluation et de traitement des risques.

3.1. But de la gestion des risques

Le but de la gestion des risques est d'identifier tous les actifs, leurs vulnérabilités et les menaces pouvant exploiter ces vulnérabilités, ainsi que d'évaluer ces paramètres afin d'établir la criticité des risques individuels.

[illegible]

3.2. Domaine d'application de l'évaluation et du traitement des risques

L'évaluation et le traitement des risques ont été réalisés au sein de [nom des unités organisationnelles], en conformité avec le Document du domaine d'application du SMSI.

3.3. Durée

Commented [AES2]: Indiquez le nom de votre organisation.

Commented [AES3]: Indiquez le nom de votre organisation.

Commented [AES4]: Vous pouvez consulter un modèle pour ce document dans le dossier "04_Domaine_d_application_du_SMSI" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES5]: Vous pouvez consulter un modèle pour ce document dans le dossier "05_Politiques_generales" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES6]: Vous pouvez consulter un modèle pour ce document dans le dossier "10_Documents_fondamentaux_sur_la_continuite_des_activites_ISO_22301" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES7]: Indiquez seulement les unités [illegible]

L'évaluation des risques a été mise en œuvre du [jour/mois/année] au [jour/mois/année]. Le traitement des risques a été mis en œuvre du [jour/mois/année] au [jour/mois/année]. Les rapports finaux ont été élaborés pendant [spécifier la période].

3.4. Participants au processus et collecte de l'information

Le processus d'évaluation et de traitement des risques a été géré par [nom et titre du poste], avec une assistance d'expert fournie par [si une assistance d'expert a été utilisée, indiquer le nom et l'entreprise].

Commented [AES8]: Par ex. Responsable continuité d'activité, [illegible]

Commented [AES9]: Vous pouvez supprimer cette partie si [illegible]

[illegible]

Commented [AES10]: Ou décrire une autre méthode utilisée.

3.5. Bref aperçu de la méthodologie appliquée

Brièvement, le processus a été mené de la manière suivante :

- tous les actifs ont été identifiés, ainsi que leurs propriétaires
- les menaces ont été identifiées pour chaque actif et les vulnérabilités correspondantes ont été identifiées pour chaque menace
- des propriétaires des risques ont été identifiés pour chaque risque
- l'impact de la perte de confidentialité, d'intégrité et de disponibilité a été évalué en utilisant des valeurs comprises entre 0 et 2
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Commented [AES11]: Supprimer ce texte si seules les mesures [illegible]

3.6. Aperçu des documents utilisés pendant le processus d'évaluation et de traitement des risques

Les documents suivants ont été utilisés ou établis au cours de la mise œuvre de l'évaluation et du traitement des risques :

- Tableau d'évaluation des risques (Annexe 1) – pour chaque combinaison d'actifs, de vulnérabilités et de menaces, ce tableau présente les valeurs d'impact et de vraisemblance, et calcule les risques
- [illegible]

4. Validité et gestion documentaire

Ce document est valide à compter du [date]. Le propriétaire de ce document est [titre du poste].

Commented [AES12]: Par ex. Responsable continuité d'activité, [illegible]

5. Annexes

- Annexe 1 – Tableau d'évaluation des risques
- [illegible]

[titre du poste]
[nom]

[signature]

Commented [AES13]: Nécessaire uniquement si la Procédure [illegible]