[logo de l'organisation]

[nom de l'organisation]

Comment [DK1]: Pour apprendre à remplir ce document, voir ce **tutoriel vidéo**: Comment écrire la méthodologie d'évaluation des risques selon ISO 27001:
- si vous avez acheté la boîte à outils, vous le trouverez dans le portail client ISO 27001 & ISO 22301: https://epps.customerhub.net/
- si vous n'avez pas acheté la boîte à outils, vous trouverez une prévisualisation du tutoriel ici: http://advisera.com/27001academy/tutorial/documentation-tutorial-how-to-write-the-iso-27001-risk-assessment-methodology/

Comment [DK2]: Pour apprendre à écrire la méthodologie, lire ces articles:
- évaluation et traitement des risques ISO 27001 – 6 étapes de base http://advisera.com/27001academy/knowledgebase/iso-27001-risk-assessment-treatment-6-basic-steps/
- Comment écrire la méthodologie d'évaluation des risques selon ISO 27001 http://advisera.com/27001academy/knowledgebase/write-iso-27001-risk-assessment-methodology/

Comment [DK3]: Tous les champs dans ce document marqués par des crochets [ ] doivent être remplis.

METHODOLOGIE D'EVALUATION ET DE TRAITEMENT DES RISQUES

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

Comment [DK4]: Le système de codage des documents devrait 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.

©2015 Ce modèle peut être utilisé par les clients de EPPS Services Ltd. www.advisera.com en conformité avec l'accord de licence.

Historique des modifications

Date	Version	Créé par	Description de la modification
JJ-MM-AAAA	0.1	Dejan Kosutic	Structure documentaire de base

Table des matières

1. BUT, DOMAINE D'APPLICATION ET AUDIENCE 3

2. DOCUMENTS REFERENCES 3

3. METHODOLOGIE D'EVALUATION ET DE TRAITEMENT DES RISQUES 3

3.1. EVALUATION DES RISQUES 3

3.1.1. Le processus 3

3.1.2. Actifs, vulnérabilités et menaces 3

3.1.3. Détermination des propriétaires des risques 4

3.1.4. Impacts et vraisemblances 4

3.2. CRITERES D'ACCEPTATION DES RISQUES 4

3.3. TRAITEMENT DES RISQUES 5

3.4. REVISIONS REGULIERES DE L'EVALUATION ET DU TRAITEMENT DES RISQUES 5

3.5. DECLARATION D'APPLICABILITE ET PLAN DE TRAITEMENT DES RISQUES 5

3.6. RAPPORTS 5

4. GESTION DES ENREGISTREMENTS CONSERVES SUR LA BASE DE CE DOCUMENT 6

5. VALIDITE ET GESTION DOCUMENTAIRE 7

6. ANNEXES 7

©2015 Ce modèle peut être utilisé par les clients de EPPS Services Ltd. www.advisera.com en conformité avec l'accord de licence.

1. But, domaine d'application et audience

Le but de ce document est de définir la méthodologie pour l'évaluation et le traitement des risques de l'information dans [nom de l'organisation], et de définir le niveau acceptable de risque, en accord avec 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 dans l'évaluation et dans le traitement des risques.

2. Documents référencés

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

Comment [DK5]: A effacer, si vous n'allez pas utiliser cette politique.

3. Méthodologie d'évaluation et de traitement des risques

Comment [DK6]: Cette méthodologie doit être modifiée si nécessaire par les exigences légales et réglementaires ou par des obligations contractuelles.

3.1. Evaluation des risques

3.1.1. Le processus

[illegible] des vulnérabilités est réalisée par les propriétaires des actifs, et l'évaluation des impacts et vraisemblances est menée par les propriétaires des risques.

Comment [DK7]: Pour simplifier le processus, [illegible] risque.

3.1.2. Actifs, vulnérabilités et menaces

La première étape dans l'évaluation des risques, est l'identification de tous les actifs dans le domaine [illegible] ou sous forme électronique, des applications et des bases de données, des personnes, des équipements ICT, l'infrastructure, et des services/processus externalisés. Lors de l'identification des [illegible] organisationnelles responsables pour chaque actif.

Comment [DK8]: [illegible]

[illegible] Les menaces et les vulnérabilités sont identifiées en utilisant les catalogues inclus dans le Tableau

©2015 Ce modèle peut être utilisé par les clients de EPPS Services Ltd. www.advisera.com en conformité avec l'accord de licence.

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 peut être ou ne pas être la même que le propriétaire de l'actif.

Comment [DK9]: Pour simplifier le processus, nous pouvons définir que le propriétaire des actifs sont chaque risque est aussi le propriétaire du risque.

3.1.4. Impacts et vraisemblances

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

Impact faible	0	Perte de confidentialité, disponibilité ou intégrité n'affectant pas le cash flow de l'organisation, ses obligations légales ou contractuelles, ou sa réputation.
Impact modéré	1	Perte de confidentialité, disponibilité ou intégrité entrainant 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, disponibilité ou intégrité, ayant un impact considérable et/ou immédiat sur le cash flow de l'organisation, sur les opérations, sur les obligations légales ou contractuelles, ou sur sa réputation.

Après l'évaluation des impacts, il est nécessaire d'évaluer la vraisemblance d'occurrence d'un tel risque, 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 robustes 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 modérés et ont essentiellement fourni un niveau de protection adéquat. De nouveaux incidents sont possibles à l'avenir.
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 entrant 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. Les mesures de sécurité existantes doivent être inscrites dans la dernière colonne du Tableau d'évaluation des risques.

3.2. Critères d'acceptation des risques

Les valeurs 0, 1 et 2 indiquent des risques acceptables, alors que les valeurs 3 et 4 indiquent des risques inacceptables. Les risques inacceptables doivent être traités.

©2015 Ce modèle peut être utilisé par les clients de EPPS Services Ltd. www.advisera.com en conformité avec l'accord de licence.

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.
Le traitement des risques est mené par [titre du poste].

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

1. Sélection des mesures de sécurité ou des mesures de l'Annexe A de la norme ISO/IEC 27001 ou d'autres mesures de sécurité.
2. Transfert des risques à un tiers - par exemple en souscrivant une police d'assurance ou en signant des contrats avec des fournisseurs ou des partenaires.
3. Eviter le risque en arrêtant l'activité commerciale à l'origine du risque.
4. Accepter le risque - cette option est autorisée que si la sélection d'autres options de traitement des risques devrait dépasser les coûts de l'impact d'un risque survenu.

La sélection des options est mise œuvre au travers du Tableau de traitement des risques. Habituellement l'option 1 est choisie - la sélection d'une ou de plusieurs mesures de sécurité. Lorsque plusieurs mesures de sécurité sont sélectionnées, des lignes supplémentaires sont insérées dans le tableau immédiatement en dessous de la ligne spécifiant le risque.

Le traitement des risques relatifs aux processus externalisés doit être adressé au travers des contrats avec le tiers concerné, comme spécifié dans la [Politique de sécurité des fournisseurs].

Comment [DK10]: A effacer si vous n'utiliserez pas cette politique.

Dans le cas de l'option 1 (sélection de mesures de sécurité), il est nécessaire d'évaluer la nouvelle valeur de l'impact et de la vraisemblance dans le Tableau de traitement des risques, pour évaluer l'efficacité des mesures planifiées.

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 ligne avec les risques nouvellement identifiés. L'examen est conduit au moins une fois par an, ou plus fréquemment dans le cas de changements organisationnels significatifs, de changements technologiques significatifs, de changements des objectifs de l'entreprise, de changements dans l'environnement des affaires, etc.

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

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

Sur la base des recommandations des propriétaires des risques, [la Direction] acceptera tous les risques résiduels au travers de la Déclaration d'applicabilité.

Comment [DK11]: Si, pour une raison quelconque, l'acceptation du risque ne fait pas partie de la Déclaration d'applicabilité (p. ex. si la Déclaration d'applicabilité est sous la responsabilité d'une autre personne que celle à la Déclaration), alors il est nécessaire de fournir ici le nom du document (décision) au travers duquel la Direction va accepter les risques résiduels.

[titre du poste] préparera le plan de traitement des risques dans lequel l'implémentation des mesures sera planifiée. Sur la base des recommandations des propriétaires des risques, [la Direction] acceptera le plan de traitement des risques.

3.6. Rapports

©2015 Ce modèle peut être utilisé par les clients de EPPS Services Ltd. www.advisera.com en conformité avec l'accord de licence.

[titre du poste] documentera les résultats de l'évaluation et du traitement des risques, et de toutes [illegible]

[titre du poste] surveillera l'avancement de l'implémentation du Plan de traitement des risques et rapportera chaque mois les résultats à [titre du poste]

Comment [DK12]: Ceci est juste une recommandation; ajuster la fréquence au besoin.

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

Nom de l'enregistrement	Lieu de conservation	Personne responsable de la conservation	Mesure de protection des enregistrements	Temps de rétention
Tableau d'évaluation des risques (forme électronique - document Excel)	Ordinateur de [titre du poste]	[titre du poste du propriétaire du Tableau d'évaluation des risques]	Seul [titre du poste] a les droits pour faire des entrées et des modifications au Tableau d'évaluation des risques	Les données sont conservées de façon permanente.
Tableau de traitement des risques (forme électronique - document Excel)	Ordinateur de [titre du poste]	[titre du poste du propriétaire Tableau de traitement des risques]	Seul [titre du poste] a les droits pour faire des entrées et des modifications au Tableau de traitement des risques	Les données sont conservées de façon permanente.
Déclaration d'Applicabilité (forme électronique - format PDF)	Ordinateur de [titre du poste]	[titre du poste du propriétaire du Rapport]	Seul [titre du poste] a les droits pour faire des entrées et des modifications à la Déclaration d'applicabilité	Les anciennes versions de la DdA sont conservées pour une période 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] a les droits pour faire des entrées et des modifications au Plan de traitement des risques	Les anciennes versions du Plan de traitement des risques sont conservées pour une période de 3 ans

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

©2015 Ce modèle peut être utilisé par les clients de EPPS Services Ltd. www.advisera.com en conformité avec l'accord de licence.

5. Validité et gestion documentaire

Ce document est valide dès le [date]

[illegible] document au moins une fois par an, avant l'examen régulier de l'évaluation des risques existants.

Comment [DK13]: [illegible]

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

- le nombre d'incidents qui se sont produits, mais ne sont pas inclus dans l'évaluation des risques
- [illegible]
- [illegible] et de traitement des risques en raison de la définition imprécise des rôles 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]

Comment [DK14]: Nécessaire uniquement si la Procédure de Contrôle des Documents et des Enregistrements prescrit que les documents papier doivent être signés.

©2015 Ce modèle peut être utilisé par les clients de EPPS Services Ltd. www.advisera.com en conformité avec l'accord de licence.