## Tableau d'évaluation des risques

implémenté du [date] au [date]

| N. | Nom de l'actif | Propriétaire de l'actif | Menace | Vulnérabilité | Propriétaire du risque | Impact | Probabilité | Risque | Mesures existantes |
|---|---|---|---|---|---|---|---|---|---|
| 1 | *administrateur système* | *responsable RH* | | | | | | *2* | |
| 2 | *logiciel d'application* | *responsable informatique* | | | | | | *3* | |
| 3 | *rapports* | *PDG* | | | | | | *2* | |
| 4 | *ordinateurs portables* | *utilisateur* | | | | | | *2* | |
| 5 | *bureaux* | *responsable des installations* | | | | | | *1* | |
| 6 | *moyens de communication* | *responsable informatique* | | | | | | *3* | |
| 7 | *administrateur système* | *responsable RH* | | | | | | *2* | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 8 | logiciel d'application | responsable informatique | | | | | | 3 | |
| 9 | logiciel d'application | responsable informatique | | | | | | 2 | |
| 10 | bureaux | responsable des installations | | | | | | 2 | |
| 11 | bureaux | responsable des installations | | | | | | 3 | |
| 12 | moyens de communication | responsable informatique | | | | | | 3 | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## Catégories d'actifs

*Les éléments suivants sont des exemples d'actifs informationnels qui peuvent être trouvés au sein de*
*Cette liste n'est pas définitive, chaque organisation doit indiquer ses propres actifs, significatifs pour l*

**Personnes**

- direction (membres du conseil d'administration, membres du conseil de surveillance, resp
- cadres moyens
- employés - experts (par ex. administrateurs système, designers, experts sécurité, etc.)
- autres employés
- employés externes à temps partiel
- personnes externes visitant l'organisation

**Applications et bases de données**

- logiciel d'application (autorisé)
- freeware ; shareware
- Logiciel système
- différents outils
- bases de données

**Documentation (sous forme papier ou électronique)**

- contrats
- correspondance avec les clients et les partenaires
- enregistrements
- journaux
- manuels
- normes
- pièces justificatives
- documentation d'équipement
- documentation de formation
- documents internes
- décisions
- rapports
- plans
- registres
- documents du personnel

**Informatique, communication et autres équipements**

- ordinateurs de bureau
- ordinateurs portables
- CD d'installation
- onduleurs
- groupes électrogènes
- climatisation
- équipements réseau
- câbles d'alimentation
- serveurs
- téléphones
- systèmes de centrale téléphonique
- téléphones mobiles

appareils PDA
imprimantes
scanners
photocopieurs
bandes de sauvegarde
support de stockage mobile
équipement de mesure
machines fax
alarmes
véhicules
cartes et lecteurs de cartes
coffres-forts
clefs

**Infrastructure**

bureaux
archives
entrepôts
coffres-forts
armoires

**Services externalisés**

alimentation électrique
moyens de communication
maintenance de l'équipement TIC
maintenance des systèmes d'information
services de courrier et de messagerie
auditeurs
consultants
institutions de contrôle

## Répertoire des menaces

*La liste suivante énumère les menaces. Cette liste n'est pas définitive. Chaque organisation peut ajou*

accès non autorisé au réseau
accès non autorisé au système d'information
accès physique non autorisé
alerte à la bombe
attaques terroristes
attentats à la bombe
autres désastres (artificiels)
autres désastres (naturels)
code malveillant
défaillance des équipements
destruction des enregistrements
détérioration des supports
détournement de fonds
divulgation de mots de passe
dommages causés par les activités de tiers
dommages subis au cours des tests d'intrusion
écoute
erreur de l'utilisateur
erreurs d'application
erreurs de maintenance
espionnage industriel
falsification de documents
feu
foudre
fraude
fuite / divulgation de renseignements
grève
ingénierie sociale
innondation
installation non autorisée de logiciels
interception d'informations
interruption de l'alimentation électrique
mauvaise utilisation des outils d'audit
mauvaise utilisation des systèmes d'information
modification non autorisée des enregistrements
modifications accidentelles des données du système d'information
pandémie, épidémie
panne des moyens de communication
perte de services d'assistance
pollution
rupture des relations contractuelles
usurpation d'identité
utilisation de codes non autorisés ou non testés
utilisation non autorisée de logiciels
utilisation non autorisée de matériels agréés
vandalisme

**Répertoire des vulnérabilités**

*La liste suivante énumère les vulnérabilités.*
*Cette liste n'est pas définitive. Chaque organisation peut ajouter des vulnérabilités spécifiques à sa si*

absence de contrôle des données d'entrée et de sortie
absence de preuve de messages envoyés ou reçus
absence de validation des données traitées
absence ou mauvaise application de l'audit interne
accès non autorisés aux installations
aucune désactivation des comptes d'utilisateurs après la cessation d'activité
clés cryptographiques accessibles aux personnes non autorisées
comptes et mots de passe générés par le système restent inchangés
connexions de réseau public non protégées
copie unique, seulement une copie de l'information
copies non contrôlées
droits d'utilisateurs insuffisants
élimination de supports de stockage sans effacer les données
employés démotivés ou mécontents
entretien inadéquat
équipement mobile sujet aux vols
exigences pour le développement de logiciels mal définies
gestion de la capacité insuffisante
gestion de réseau insuffisante
gestion du changement insuffisante
informations accessibles à des personnes non autorisées
interface utilisateur compliquée
logiciels non-documentés
mauvaise sélection des données de test
mauvaises conditions d'hygiène
mots de passe faibles
niveau de confidentialité mal défini
niveau insuffisant de connaissance et/ou de sensibilisation des employés
obsolescence des bases de données pour la protection contre les codes malveillants
pas de séparation des environnements de test et de production
placements des câbles
pouvoirs étendus
règles cryptographiques mal définies
règles d'organisation mal définies
règles pour le contrôle d'accès mal définies
règles pour travailler hors des bureaux mal définies
répartition inadéquate des tâches
réseaux accessibles aux personnes non autorisées
sensibilité de l'équipement à la température
sensibilité de l'équipement à l'humidité et à la pollution
sensibilité de l'équipement aux variations de tension
sessions actives après les heures de travail
site sensible aux catastrophes naturelles
site sensible aux fuites d'eau
supervision inadéquate du travail des employés

supervision insuffisante des fournisseurs externes
sur-dépendance à un appareil / système
systèmes non protégés contre tout accès non autorisé
téléchargements sur Internet non contrôlés
utilisation de matériel ancien
utilisation non contrôlée des systèmes d'information