Traiter les risques M 23

|  |  |
| --- | --- |
| type | processus de management |
| finalité | * atteindre les objectifs du SMSI * choisir les options de traitement des risques de sécurité de l’information * élaborer un plan de traitement des risques de sécurité de l’information * protéger la confidentialité, la disponibilité et l’intégrité des actifs * améliorer la performance globale de l’entreprise |
| pilote | directeur / responsable sécurité de l’information / chef de projet |
| risques | * ne pas prendre en compte le contexte de l’entreprise * ne pas choisir les options de traitement des risques * ne pas déterminer les mesures de traitement des risques * ne pas mettre en place les mesures de traitement des risques * ne pas élaborer le plan de traitement des risques * ne pas fournir les ressources nécessaires * ne pas attribuer les responsabilités * ne pas communiquer sur les risques aux parties intéressées * ne pas déclencher les mesures face aux risques identifiés * ne pas produire la déclaration d’applicabilité |
| processus amont | * apprécier les risques * planifier le SMSI * piloter les processus |
| processus aval | * réaliser la revue de direction * communiquer * satisfaire aux exigences |
| éléments d'entrée | * contexte de l’entreprise * ressources nécessaires * conditions (normales et anormales) * tout risque identifié |
| activités  (sous-processus) | * choisir les options de traitement des risques (éviter, réduire, accepter, partager) * déterminer les mesures nécessaires pour traiter les risques * vérifier les mesures déterminées avec celles de l’Annexe A de l’ISO 27001 * établir la déclaration d’applicabilité * élaborer le plan de traitement des risques * attribuer les responsabilités pour le plan de traitement des risques * faire accepter les risques résiduels * conserver les informations documentées sur le traitement des risques * communiquer |
| éléments de sortie | * plan d'action (mesures de traitement des risques) * surveillance des mesures de traitement des risques * risques résiduels * sensibilisation du personnel |
| ressources | direction, responsables départements, pilotes processus, chefs de projet |
| indicateurs | * indicateurs clés de performance (*KPI – key performance indicators)* * risques traités * actions mises en place |
| procédures / documents | amélioration continue, communication, planification, gestion des changements, maîtrise des processus, inspection / liste des risques, déclaration d’applicabilité, plans de traitement des risques, fiches processus, enquête de satisfaction clients, demandes de changement, rapports |
| clients | l’ensemble du personnel et des processus, parties intéressées |

Glossaire :

SMSI : système de management de la sécurité de l’information

KPI : indicateurs clés de performance (*key performance indicators)*

* atteindre les objectifs du SMSI
* choisir les options de traitement des risques de sécurité de l’information
* élaborer un plan de traitement des risques de sécurité de l’information
* protéger la confidentialité, la disponibilité et l’intégrité des actifs
* améliorer la performance globale de l’entreprise

directeur / responsable sécurité de l’information / chef de projet

traiter les risques /

M 23

titre / codification

finalité

pilote

risques

processus amont

processus aval

* ne pas prendre en compte le contexte de l’entreprise
* ne pas choisir les options de traitement des risques
* ne pas déterminer les mesures de traitement des risques
* ne pas mettre en place les mesures de traitement des risques
* ne pas élaborer le plan de traitement des risques
* ne pas fournir les ressources nécessaires
* ne pas attribuer les responsabilités
* ne pas communiquer sur les risques aux parties intéressées
* ne pas déclencher les mesures face aux risques identifiés
* ne pas produire la déclaration d’applicabilité
* apprécier les risques
* planifier le SMSI
* piloter les processus
* réaliser la revue de direction
* communiquer
* satisfaire aux exigences

éléments de sortie

activités

éléments d'entrée

* choisir les options de traitement des risques (éviter, réduire, accepter, partager)
* déterminer les mesures nécessaires pour traiter les risques
* vérifier les mesures déterminées avec celles de l’Annexe A de l’ISO 27001
* établir la déclaration d’applicabilité
* élaborer le plan de traitement des risques
* attribuer les responsabilités pour le plan de traitement des risques
* faire accepter les risques résiduels
* conserver les informations documentées sur le traitement des risques
* communiquer
* plan d'action (mesures de traitement des risques)
* surveillance des mesures de traitement des risques
* risques résiduels
* sensibilisation du personnel
* contexte de l’entreprise
* ressources nécessaires
* conditions (normales et anormales)
* tout risque identifié

clients

procédures / documents

indicateurs

ressources

amélioration continue, communication, planification, gestion des changements, maîtrise des processus, inspection / liste des risques, déclaration d’applicabilité, plans de traitement des risques, fiches processus, enquête de satisfaction clients, demandes de changement, rapports

indicateurs clés de performance,

risques traités,

actions mises en place

l’ensemble du personnel et des processus, parties intéressées

direction, responsables départements, pilotes processus, chefs de projet