Passer en revue la sécurité R 65

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | assurer la pertinence, l’adéquation et l’efficacité de la gestion de la sécurité de l’information au moyen d’une revue indépendante |
| pilote | responsable sécurité de l’information |
| risques | * ne pas planifier des revues du SMSI * ne pas passer en revue régulièrement la sécurité de l’information * ne pas auditer le SMSI * ne pas saisir des opportunités d’amélioration du SMSI * ne pas réaliser des tests d’audit du SMSI * ne pas passer en revue les politiques, les mesures de sécurité, les processus et les procédures * ne pas passer en revue la sécurité suite à :   + des changements de la loi   + un incident significatif   + au démarrage d’un nouveau produit   + un changement du SMSI (politique, procédure) * ne pas entreprendre des actions correctives |
| processus amont | * planifier le SMSI * apprécier les risques * traiter les risques * auditer |
| processus aval | * gérer la chaîne TIC * satisfaire aux exigences de la sécurité * tester * appliquer la sécurité * réaliser des actions correctives |
| éléments d'entrée | * plan de traitement des risques * plan de gestion des incidents * événements de sécurité de l’information * plan de gestion des changements |
| activités  (sous-processus) | * planifier des revues du SMSI * passer en revue régulièrement la sécurité de l’information * auditer le SMSI * saisir des opportunités d’amélioration du SMSI * réaliser des tests d’audit du SMSI * passer en revue les politiques, les mesures de sécurité, les processus et les procédures * passer en revue la sécurité suite à :   + des changements de la loi   + un incident significatif   + au démarrage d’un nouveau produit   + un changement du SMSI (politique, procédure) * entreprendre des actions correctives |
| éléments de sortie | * résultats des revues de sécurité * rapport d’action corrective * résultats des actions correctives |
| ressources | moyens techniques et informatiques |
| indicateurs | * nombre de revues passées à temps * nombre d’opportunités d’amélioration saisies |
| procédures / documents | chaîne TIC, activités de surveillance, incidents, changements / registre des incidents, plan de traitement des risques, plan de gestion des incidents, événements de sécurité de l’information, plan de gestion des changements, résultats des surveillances et des mesures, résultats des revues de sécurité, rapport d’action corrective, résultats des actions correctives |
| clients | auditeurs |

Glossaire :

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

TIC : technologie de l’information et de la communication

assurer la pertinence, l’adéquation et l’efficacité de la gestion de la sécurité de l’information au moyen d’une revue indépendante

responsable sécurité de l’information

passer en revue la sécurité / R 65

processus amont

risques

processus aval

* gérer la chaîne TIC
* satisfaire aux exigences de la sécurité
* tester
* appliquer la sécurité
* réaliser des actions correctives
* planifier le SMSI
* apprécier les risques
* traiter les risques
* auditer
* ne pas planifier des revues du SMSI
* ne pas passer en revue régulièrement la sécurité de l’information
* ne pas auditer le SMSI
* ne pas saisir des opportunités d’amélioration du SMSI
* ne pas réaliser des tests d’audit du SMSI
* ne pas passer en revue les politiques, les mesures de sécurité, les processus et les procédures
* ne pas passer en revue la sécurité suite à :
  + des changements de la loi
  + un incident significatif
  + au démarrage d’un nouveau produit
  + un changement du SMSI (politique, procédure)
* ne pas entreprendre des actions correctives

éléments de sortie

éléments d'entrée

activités

* planifier des revues du SMSI
* passer en revue régulièrement la sécurité de l’information
* auditer le SMSI
* saisir des opportunités d’amélioration du SMSI
* réaliser des tests d’audit du SMSI
* passer en revue les politiques, les mesures de sécurité, les processus et les procédures
* passer en revue la sécurité suite à :
  + des changements de la loi
  + un incident significatif
  + au démarrage d’un nouveau produit
  + un changement du SMSI (politique, procédure)
* entreprendre des actions correctives
* résultats des revues de sécurité
* rapport d’action corrective
* résultats des actions correctives
* plan de traitement des risques
* plan de gestion des incidents
* événements de sécurité de l’information
* plan de gestion des changements

procédures / documents

clients

indicateurs

ressources

chaîne TIC, activités de surveillance, incidents, changements / registre des incidents, plan de traitement des risques, plan de gestion des incidents, événements de sécurité de l’information, plan de gestion des changements, résultats des surveillances et des mesures, résultats des revues de sécurité, rapport d’action corrective, résultats des actions correctives

auditeurs

nombre de revues passées à temps, nombre d’opportunités d’amélioration saisies

moyens techniques et informatiques