AIDE-MÉMOIRE

RÉALISER UN AUDIT DE SÉCURITÉ

Objectif du document

Même si vous avez de bonnes connaissances en sécurité et que vous vous tenez à l'affût de l'actualité dans ce domaine, rien ne vaut l'avis ou l'opinion d'un expert externe pour vous donner l'heure juste.

Ce document vous aidera à déterminer quel type d'audit sécurité choisir et comment vous y préparer.

Destinataire du document : Gestionnaire et personne responsable de la sécurité des systèmes d'information.

Date de la dernière modification : 2018-05

Pourquoi faire un audit de sécurité ?

Des bénéfices pour l'organisation

Il existe de nombreux bénéfices tangibles à faire un audit de sécurité. Voici quelques exemples :

- Identifier les forces et faiblesses de vos mesures de sécurité en place
- Profiter de la connaissance de ressources spécialisées en sécurité qui donneront des avis et des conseils spécifiques à votre organisation et à votre secteur d'activités
- Sensibiliser la haute direction sur l'existence des mesures de contrôle, leur mise en application et l'efficacité de leur fonctionnement
- Rassurer vos clients au sujet de la gouvernance de votre organisation en matière de sécurité
- Vous démarquer de vos compétiteurs et répondre à des appels d'offres pour lesquels cela devient une exigence

Utilisation d'un auditeur indépendant externe

L'autoévaluation des mesures de sécurité est possible, mais de faire appel à un auditeur indépendant externe permet d'assurer une plus grande crédibilité du travail effectué. Le choix de l'auditeur dépend du type de rapport.

Différents types d'audit

Un rapport d'audit de sécurité peut répondre à un ou plusieurs besoins. Ces besoins peuvent être :

- **Réglementaire**
  Selon le secteur d'activités dans lequel vous œuvrez, les autorités réglementaires peuvent demander ou exiger un rapport d'audit de sécurité;
- **Financier**
  Dans le cadre de la préparation des états financiers, les auditeurs demanderont un rapport d'audit pour les fournisseurs de services externes à l'organisation;
- **Réputationnel**
  Pour faire la démonstration que vous faites une bonne gestion de vos risques et contrôles technologiques;
- **Crédibilité**
  Afin de rassurer la direction de votre organisation, un rapport d'audit contenant une opinion externe est une source de crédibilité;
- **Commercial**
  Puisque la connaissance au sujet de la sécurité est devenue un des critères pour le choix des fournisseurs de produits et services, cela vous permettra de répondre à un appel d'offres à titre de fournisseurs de biens et services.

Les types de rapports

Il existe plusieurs types de rapports d'audit se rapportant à des normes différentes. Il y a la série de rapports SOC (*System and Organization Controls*), ISO / IEC 27 001 ou encore les audits spécialisés.

Voici un tableau qui résume les appellations, les organisations autorisées à émettre le rapport, la portée, les objectifs et les destinataires de chacun des rapports.

Tableau 1 : Les différents rapports d'audit

Nom du rapport d'audit	Objectifs et finalité du rapport d'audit	Organisation autorisée à émettre le rapport
SOC 1[1]	Démontrer l'adéquation des contrôles pertinents pour répondre aux audits financiers ou aux exigences de divulgation financière (ex. : SOX, règlement 52-109). Permet d'obtenir une opinion émise par un auditeur externe indépendant sur la conception et la mise en application des contrôles (type 1) et l'efficacité du fonctionnement des contrôles (type 2).	Firmes comptables
SOC 2	Démontrer l'adéquation des contrôles pertinents pour la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité et la protection des renseignements personnels. Permet d'obtenir une opinion émise par un auditeur externe indépendant sur la conception et la mise en application des contrôles (type 1) et l'efficacité du fonctionnement des contrôles (type 2).	Firmes comptables
SOC 3	Basé sur les *Trust Services Principles*, est surtout utilisé pour démontrer l'existence des contrôles et à des fins marketing.	Firmes comptables
ISO / IEC 27 001	Permet d'obtenir une évaluation sur la mise en place d'un système de *management* de la sécurité de l'information en respect avec les critères de la norme ISO 27002.	Firmes ou des personnes possédant l'expertise et accréditées peuvent émettre ce type de rapport
Audits spécialisés (ex. : PCI-DSS)	Permet d'obtenir une évaluation et le résultat d'analyses pour certains éléments liés à la sécurité, comme les tests de vulnérabilités, la découverte de failles et le respect de la norme PCI-DSS.	Firmes professionnelles ou des personnes ayant une expertise technique de pointe en sécurité peuvent émettre ce type de rapport

[1] Le SOC 1 est aussi nommé SSAE-18 ou NCMC 3416

Grandes étapes d'un audit

Avant l'audit

Pour les gestionnaires

- Prévoir les ressources nécessaires (personnel, budget, etc.)
- Autoriser la tenue de l'audit (engagement contractuel de l'auditeur)
- Déterminer l'étendue des services à auditer
- Informer le conseil d'administration

Pour les employés

- Collaborer à déterminer l'étendue des services à auditer
- Planifier les activités pour accompagner l'auditeur
- Préparer la documentation nécessaire

Pendant l'audit

Pour les gestionnaires

- Obtenir un suivi périodique du déroulement de l'audit et des lacunes potentielles décelées

Pour les employés

- Accompagner l'auditeur afin de faciliter son travail

Après l'audit

Pour les gestionnaires

- Prendre connaissance du rapport et le signer
- Faire le post-mortem et documenter les pistes d'amélioration

Pour les employés

- Distribuer les rapports aux demandeurs
- Élaborer et suivre les plans d'action, s'il y a lieu

Comment bien s'y préparer

Une bonne préparation permet de réduire les coûts, faciliter le travail de l'auditeur et réduire les écarts. Voici les activités à réaliser pour bien vous préparer à un audit de sécurité.

- Établir les besoins de l'organisation; cela déterminera le type d'audit et de rapport à émettre
- Au préalable, faire une autoévaluation des mesures de contrôle faisant l'objet de l'audit
- Bien planifier la période de l'année et la disponibilité des ressources
- Établir la portée (étendue) des services à auditer

- Faire un budget (coût de l'audit incluant les efforts des personnes impliquées)
- S'assurer qu'au moins une personne à l'interne ait les connaissances
- Éviter d'engager une personne ou une firme qui n'a pas les connaissances requises (même votre auditeur comptable actuel n'a peut-être pas les connaissances en ce domaine)

Pour aller plus loin

Quelques références pratiques :

- Site de l'AICPA, au sujet du SOC (en anglais)
  https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html

- Site de l'organisation mondiale de normalisation (ISO) au sujet de la norme ISO / IEC 27001 : https://www.iso.org/fr/isoiec-27001-information-security.html

- Quelques firmes comptables qui peuvent émettre des rapports SOC et spécialisées en sécurité (liste non exhaustive) :
  - PwC : www.pwc.com/ca/fr.html
  - Deloitte : https://www2.deloitte.com/ca/fr.html
  - E&Y : http://www.ey.com/home
  - KPMG : https://home.kpmg.com/ca/fr/home.html
  - BDO : www.bdo.ca

- Autres firmes professionnelles spécialisées en sécurité (liste non exhaustive) :
  - Infidem : https//infidem.biz/
  - GoSecure : http://gosecure.net/fr/
  - MNP : http://www.mnp.ca/