Institut des auditeurs internes de Québec
ISACA - Section Québec

À chacun son rapport SOC

Le bon rapport au bon endroit

Présenté par Marc Fournier, associé, PwC
Le 12 avril 2022

Table des matières

Un rapport d'audit sur les contrôles

La responsabilité des contrôles ne peut pas être déléguée

Aujourd'hui, il est de plus en plus courant pour les entreprises **d'externaliser certaines fonctions** entières à des sociétés de services. Cependant, lors de l'externalisation de ces fonctions, de nombreux risques de la société de services deviennent également les risques des entreprises utilisant les sociétés de services.

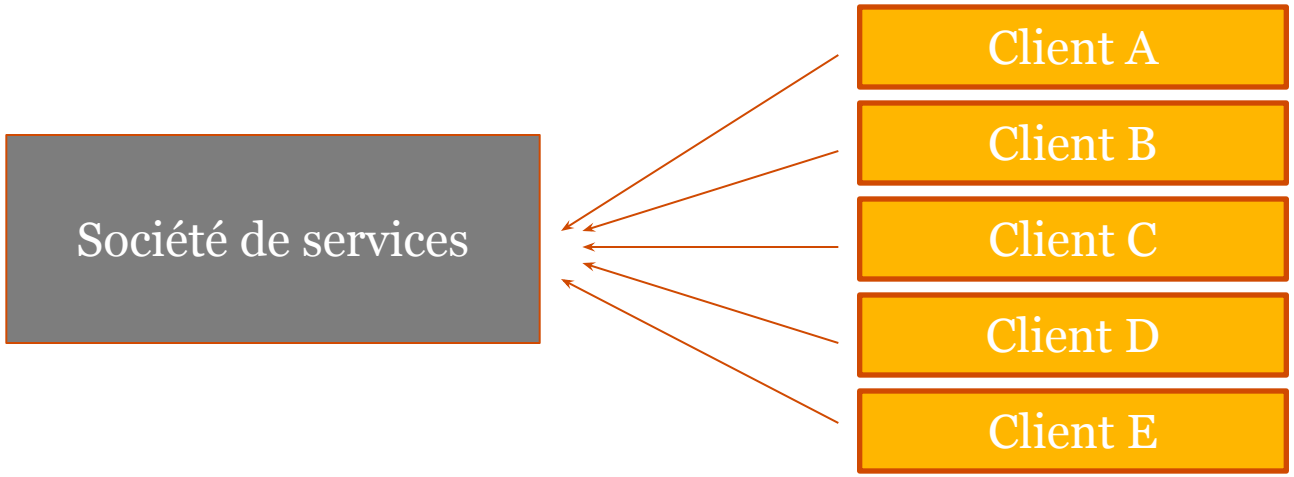
Alors que la direction peut déléguer des tâches ou des fonctions à une société de services, **la responsabilité des contrôles ne peut pas être déléguée.**

L'obtention d'un rapport indépendant sur les contrôles (SOC 1 ou SOC 2) permet à la direction de gérer sa responsabilité envers ses contrôles externalisés.

SOC report = System & Organisation Controls report

Pourquoi un rapport sur les contrôles ?

Multiple demandes de clients



Distribution d'un seul rapport

Quels sont les bénéfices d'un rapport sur les contrôles ?

- Réduction du nombre de demandes de clients et d'audits potentiels.
- Réduction du temps consacré aux divers audits et aux diverses demandes.
- Donne une assurance indépendante que les processus et contrôles sont exercés de façon contrôlée.
- Permet de communiquer clairement les mises à jour et les améliorations de systèmes, processus et contrôles, lors de changements.

Bénéfices d’un rapport SOC

Bénéfices pour la société de services (émetteur)

- Gestion des coûts
- Différentiation dans le marché
- Conscience de contrôle accrue au sein de l'organisation
- Personnalisable pour le respect de divers cadres d'atténuation des risques (SOC 2)

Bénéfices pour la société utilisatrice du rapport SOC (client)

- Opinion d'un tiers indépendant portant sur le contrôle interne couvrant les besoins d'information de l'utilisateur
- Gain de temps et d'argent grâce à la réduction et/ou à l'élimination des audits sur site et du processus de questionnaire
- Gain de temps lors de la revue diligente de la société de service et du suivi/surveillance en continu
- Mécanisme de mesure cohérente et uniforme lors de l'évaluation des prestataires de services par rapport aux risques critiques
- Rapports détaillés sur l'environnement de contrôle global de la société de services (SOC 2)

Rapports SOC 1 -> États financiers du client

Un mission réalisée selon la norme NCMC 3416 est appelé une mission SOC 1.

Les rapports SOC 1 se concentrent **uniquement** sur les systèmes et les contrôles de la société de services qui peuvent être **pertinents pour les contrôles internes des entités utilisatrices à l'égard de l'information financière.**

Ces rapports sont fréquemment demandés aux organisations de services car ils sont nécessaires pour l'audit des états financiers des entités utilisatrices. Exemples d'organisations de services pouvant fournir un rapport SOC1 :

- Sociétés de traitement de la paie
- Sociétés de traitement des prestations de santé
- Services fiduciaires des banques et des compagnies d'assurance
- Gestionnaire de portefeuille
- Gestion logistique du numéraire
- Services de billetterie
- Fournisseur de logiciel applicatif
- Fournisseur TI supportant des applications financières

Rapports SOC 2 -> Sécurité

Les rapports SOC 2 sont appropriés pour les missions de rapport sur les contrôles d'une société de services liés aux services Trust, définis par l'AICPA. Les services Trust sont :

- Sécurité
- Disponibilité
- Intégrité du traitement
- Confidentialité
- Protection des renseignements personnels

** Les missions SOC 2 sont exécutées conformément norme d'attestation NCMC 3000 en utilisant les directives du guide AICPA *Rapports sur les contrôles au sein de l'organisation de service relatifs à la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité ou la protection des renseignements personnels (SOC 2).*

Rapports SOC 3 -> très rare - aucun au Canada

Rapports sur les contrôles - Sommaire

	SOC 1	SOC 2
Objectif du rapport	**Donner aux auditeurs des états financiers des clients** de la société de services de l'information à propos des contrôles de la société de services qui sont **pertinents pour le contrôle interne à l'égard de l'information financière de ses clients** utilisateurs.	**Donner à la direction de la société de services, ses clients utilisateurs, et autres parties convenues** des informations et une opinion indépendante des contrôles de la société de services **pertinents pour la sécurité, la disponibilité, l'intégrité des traitements, la confidentialité ou la protection des renseignements personnels.**
Champs d'application	Contrôles **pertinents pour le contrôle interne à l'égard de l'information financière** des entités utilisatrices (clients)	Contrôles **pertinents pour (au choix) la Sécurité (obligatoire), Disponibilité, Intégrité des traitements, Confidentialité, Protection des renseignements personnels**
Contenu du rapport	1. Opinion de l'auditeur sur: i. Fidélité de la présentation de la description ii. Conception des contrôles (Type I et II) iii. Efficacité des contrôles ((Type II seulement) 2. Déclaration de la direction 3. Description du système de la société de service 4. Description des contrôles, des tests de l'auditeur et résultats 5. Information additionnelle (non auditée)	
Norme d'audit	Canada: NCMC 3416 - Rapport sur les contrôles d'une société de services pertinent pour la divulgation de l'information financière. États-Unis : AT-C 320 (aussi appelé SSAE 18 anciennement SSAE 16) International : ISAE 3402	Canada: NCMC 3000 - Missions d'attestation autres que les audits ou examens d'informations financières historiques États-Unis: AT-C 205 et critères Trust de l'AICPA International: ISAE 3000

Critères SOC 2 (1/2)

Catégories		Sections	Nombre de critères
Sécurité	COSO	CC1- Environnement de contrôle	5
		CC2- Communication et Information	3
		CC3- Évaluation des risques	4
		CC4- Activités de surveillance	2
		CC5- Activités de contrôle	3
		CC6- Contrôles d'accès logiques et physiques	8
		CC7- Opérations de systèmes	5
		CC8- Gestion des changements	1
		CC9- Atténuation de risques	2
Disponibilité			3
Confidentialité			2
Intégrité de processus			5

Habituellement 80 à 100 contrôles requis pour atteindre les critères

De 10 à 20 contrôles additionnels requis

Critères SOC 2 (2/2)

Catégories	Sections	Nombre de critères
Protection des renseignements personnels (Privacy)	P1- Notice et communication des objectifs	1
	P2- Choix et consentement	1
	P3- Collecte	2
	P4- Utilisation, rétention et disposition	3
	P5- Accès	2
	P6- Divulgation et notification	7
	P7- Qualité	1
	P8- Surveillance et mise en application	1

Environ 50 contrôles additionnels requis pour atteindre les critères reliés à la catégorie “Privacy”

Les critères requis pour cette catégorie sont intimement liés à la loi 64 du Québec et au règlement GDPR en Europe.

Nouveaux types de rapports SOC et tendances futures (1/2)

SOC 2+

- SOC 2 jumelé à un autre cadre de référence
- Multi-conformité
- AICPA a développé certains « mappings »:
  - ISO 27001
  - NIST CSF
  - COBIT 5
  - NIST 800-53
  - GDPR

Nouveaux types de rapports SOC et tendances futures (2/2)

SOC 2 sur la cybersécurité

- Flexibilité sur le cadre de contrôle à utiliser (ISO 27001, NIST, TSC, etc.)
- Rapport pouvant être émis pour des fins internes (vs sociétés de services pour SOC 1-2)
- Obligations règlementaires d'évaluation des profiles de risques de cybersécurité pour les institutions financières ayant des opérations dans l'état de New York

SOC sur la chaîne d'approvisionnement

- Système visé: Production, fabrication ou distribution de produits – TSC applicables
- Rapport est aussi conçu pour fournir de l'information pouvant être utilisé à identifier, évaluer et gérer les risques en lien avec les relations entre les entités.

Rapports de sécurité -> SOC 2 vs ISO 27001

Points communs :

- Périmètre : les deux démarches adressent la sécurité, la confidentialité, l'intégrité et la disponibilité des données. 96% des contrôles de sécurité sont communs
- Même usage et acceptation par l'écosystème
- Sont réalisés par des firmes indépendantes
- Coûts comparables, mais…
- Renouvellement périodique

Différences :

- ISO est une **certification**, SOC est un **audit** (opinion) - Opinion plus forte car test l'efficacité opérationnelle et non seulement la mise en place.
- ISO27001 est historiquement plus présent en Europe malgré une grande percée du SOC 2 en Europe.
- ISO27001 ne peut être accrédité que par un organisme certifié (PwC Canada est certifié)
- Plus coûteux de mettre en place une certification ISO27001 qu'un SOC 2
- Certification annuelle est plus coûteuse pour le SOC 2 car test l'efficacité opérationnelles des contrôles à tous les ans. Par contre, plus grande assurance obtenue.

Calendrier typique (échéancier rapide) - Rapport SOC 2