Survivre au SOC2 !

Présentation à la conférence SéQCure 2019

8 avril 2019

Desjardins

Votre présentateur

- Denis Jolin CPA, CA, CA-TI, CITP, CISA, CISSP
- 26 d’expérience comme auditeur (15 ans en audit TI)
- Chez Desjardins depuis mars 2010
- Gestionnaire responsable de l’équipe Risques et conformité TI

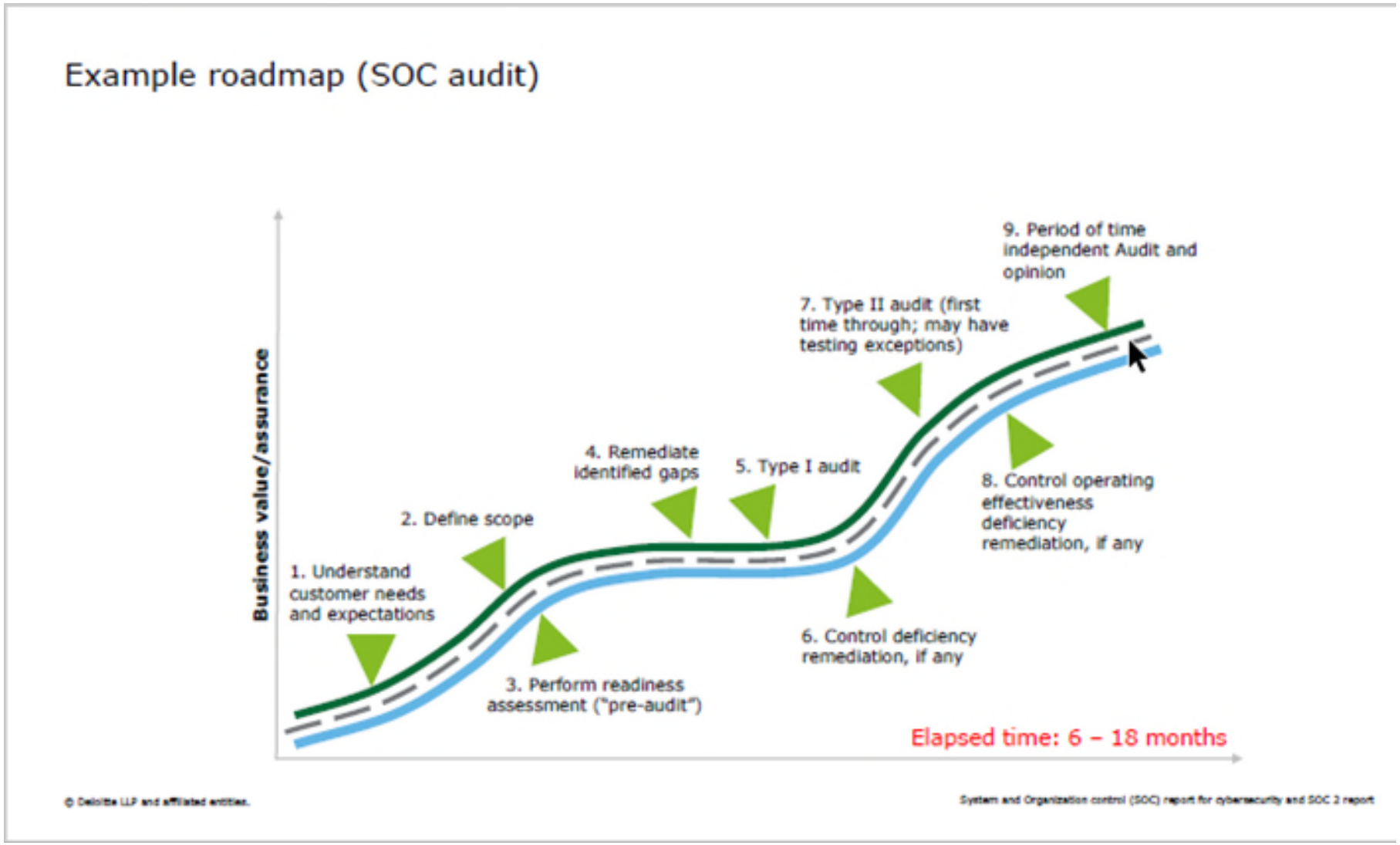
Rapports « *Service Organization Control* » : « SOC1 », « SOC2 » et « SOC3 »

	Rapport SOC1	Rapport SOC2	Rapport SOC3
Normes professionnelles	NCMC 3416 SSAE 18 ISAE 3402	CPA Canada 3001 AT 101	CPA Canada 3001 AT 101
Sujet	Contrôles pertinents pour le contrôle interne de l'information financière	Contrôles pertinents pour la sécurité, disponibilité, intégrité des traitements, confidentialité ou vie privée	Contrôles pertinents pour la sécurité, disponibilité, intégrité des traitements, confidentialité ou vie privée
But	Supporter les audits d'états financiers des entités utilisatrices	Fournir une opinion à savoir si les principes des services Trust sont rencontrés	Fournir une opinion à savoir si les principes des services Trust sont rencontrés
Entités utilisatrices	Usage restreint – la direction de la société de services, la direction des entités utilisatrices, les auditeurs des entités utilisatrices	Usage généralement restreinte – parties qui connaissent les services, les interactions, le contrôle interne et les critères	Rapports à des fins d'utilisation générale.

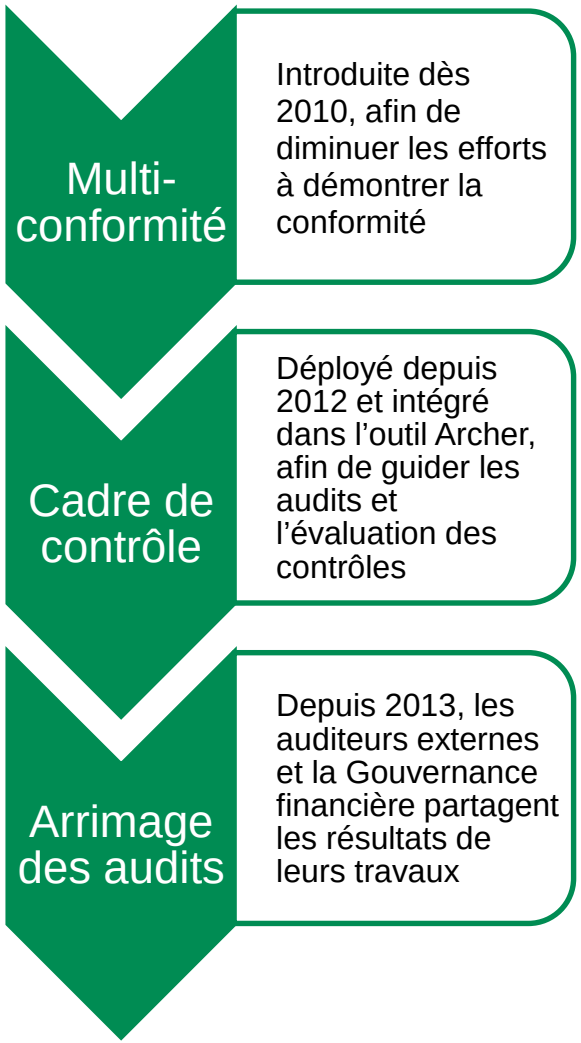
Environnement technologique Desjardins pour le mandat SOC2

	Global	Audit SOC2
Applications	1 323	156
Contrôles technologiques	263	77
Employés	4 500	30
Consultants	1 000	0
Nombre demandes (audit)	?	2 000

Cheminement SOC2



1. Comprendre les besoins
Une suite logique…de conformité



1 500 contrôles

Variation selon les besoins des demandeurs

Posséder son propre cadre de contrôle technologique est intéressant, mais demande une vigie en continu

Économie de coûts et d'efforts autant pour les auditeurs que les audités

La suite : obtenir un rapport d'audit sur les contrôles, un moyen efficace de répondre à plusieurs demandes…

1. Comprendre les besoins
Les choix à faire

Pourquoi un rapport SOC2?

- Arrimage des audits et des évaluations de contrôle
- Transparence envers la haute direction
- Répondre aux demandes de clients (questionnaire de sécurité)
- Répondre à des appels d’offres (le SOC2 devient une quasi-obligation)

1. Comprendre les besoins

La théorie

- La haute direction :
  - définit les besoins
  - détermine les utilisateurs
  - établit les conditions
  - met en place l'organisation nécessaire pour livrer le rapport
  - fournit la liste des contrôles pour atteindre les objectifs

La réalité

- Les besoins émanent le plus souvent du terrain
- Il faut influencer la direction et souvent les éduquer

À retenir

- Prendre le temps de recenser tous les besoins
- Former la haute direction
- Lire l'aide-mémoire ***Réaliser un audit de sécurité*** (trousse de cybersécurité sur le site desjardins.com)

2. Définir l’étendue
Les choix à faire

Critères

- Sécurité (critères communs)
- Confidentialité
- Disponibilité
- Intégrité du traitement
- Protection des renseignements personnels

Date

- Déterminée en fonction des besoins des utilisateurs
- Plusieurs combinaisons possibles (à une date précise, 1 an, 10 mois, 2 périodes de 6 mois, etc.)

Tiers

- Méthode d’inclusion ou d’exclusion des sous-traitants?

2. Définir l’étendue

La théorie

- Selon les critères de 2016, 5 domaines de principes Trust
- Selon les critères de 2017, se base sur les critères de COSO
- Tous les critères sont importants pour l’organisation

La réalité

- Utilisation de 4 des 5 domaines Trust (nous n’avons pas choisi la PRP)
- Nous évaluons les critères de 2017 à utiliser
- Travail sur les textes a été très long et très exigeant
- Contrôles non connus (non audités)

À retenir

- Limiter le nombre de critères à utiliser
- Limiter le nombre d’applications
- Y aller de façon progressive
- Ne pas traiter le volet de PRP avant d’avoir une grande maturité dans l’organisation

3. et 4. Faire un pré-audit et corriger les lacunes

La théorie

- Étape FORTEMENT recommandée
- Permet de déceler les lacunes importantes

La réalité

- Grand nombre d’années d’audit et de gestion de la multiconformité
- Plusieurs constatations et recommandations en cours de règlement
- Nous n’avons pas fait de pré-audit

À retenir

- OBLIGATOIRE si vous n’avez pas une vue complète
- Permet de prendre une décision éclairée sur la suite

5. Rapport type 1

- À une date précise
- Permet de définir si la conception et la mise en œuvre des contrôles sont adéquates
- L'auditeur émet un rapport formel en se basant sur le travail effectué
- Le rapport ne contient pas la description des tests que l'auditeur a effectué

Les composantes d'un rapport SOC 2 type 1 sont les suivantes :

- Rapport des auditeurs
- Déclaration de la direction sur l'environnement de contrôle
- Description de l'organisation et des contrôles qui seront audités
- Description des critères Trust et des contrôles audités
- Résultat du travail de l'auditeur

5. Rapport type 1

La théorie

- Le rapport est complet et doit comprendre toutes les sections prescrites
- Ce type de rapport ne répond pas à tous les besoins
- Le rapport ne peut être utilisé pour démontrer l'efficacité du fonctionnement des contrôles

La réalité

- Rapport émis en date du 31 octobre 2017
- Rapport publié le 30 avril 2018
- Un travail énorme pour établir la description
- L'arrimage entre les TSP et les contrôles est un travail de moine

À retenir

- Utiliser le pré-audit pour bien établir l'étendue de l'audit
- Se préparer adéquatement :
  - Maîtriser la description de l'environnement
  - Les propriétaires des contrôles doivent bien les connaître
  - Les personnes qui ont la responsabilité de produire le rapport doivent être dédiées à cette tâche

6. Corriger le déficiences de conception

La théorie

- La conception et la mise en œuvre des contrôles est la base pour déterminer si le fonctionnement des contrôles sera adéquat

La réalité

- Résultat de notre audit :
  - Peu de déficiences de conception
  - Pas de déficiences de conception dans les secteurs névralgiques (sécurité, exploitation gestion des changements)

À retenir

- Une analyse minutieuse de ce type de déficience est primordiale
- Ne pas prendre pour acquis que sans déficience de conception tous les contrôles seront efficaces
- Le rapport peut ne pas être publié si trop de déficiences

7. Rapport type 2

- Pour une période choisie (ne peut être moins de six mois)
- Permet de définir si la conception, la mise en œuvre et l'efficacité du fonctionnement des contrôles sont adéquates
- L'auditeur émet un rapport formel en se basant sur le résultat des tests effectués

Les sections d'un rapport SOC 2 type 2 sont les suivantes :

- Rapport de l'auditeur
- Déclaration de la direction sur l'environnement de contrôle
- Description de l'organisation et des contrôles qui seront audités
- Description des critères Trust et des contrôles audités
- Résultat du travail de l'auditeur, y compris la constatation des déficiences
- Plans d'action de l'organisation en lien avec les déficiences constatées (non audité)

7. Rapport type 2

La théorie

- Le rapport est complet et doit comprendre toutes les sections prescrites
- Le rapport est utilisé pour démontrer l'efficacité du fonctionnement des contrôles
- Les contrôles ayant déjà fait l'objet d'une évaluation ou d'un audit

La réalité

- Quelques équipes n'avaient jamais été auditées; ce qui a causé une commotion
- Modification ou ajustement du libellé du contrôle (plus de 40 contrôles)
- Même avec une grande expérience en audit, 16 contrôles ont fait l'objet d'une déficience d'efficacité

À retenir

- Être capable d'expliquer le fonctionnement d'un contrôle de bout en bout
- Ne pas négliger les efforts pour bien comprendre le fonctionnement d'un contrôle et l'expliquer à l'auditeur
- Le rapport peut ne pas être publié s'il y a trop de déficiences

8. Corriger les déficiences d’efficacité

La théorie

- Peut permettre de revoir un processus, des procédures, le cheminent de l’information, etc.
- A un impact sur le respect de l’échéancier

La réalité

- Lien très étroit entre les déficiences connues et celles constatées dans le rapport
- À l’émission du rapport, 6 des 16 contrôles déficients avaient été corrigés

À retenir

- Ne pas négliger le temps requis pour corriger une déficience (parfois de plusieurs mois à plus d’un an)
- Pendant la correction, la période d’audit subséquente est débutée et les contrôles sont toujours déficients!

9. Émettre le rapport

La théorie

- L’adéquation des contrôles aux principes Trust doit être sans faille
- Des retards par rapport à l’échéancier prévu sont fréquents, mais peuvent avoir des conséquences
- Le rapport de l’auditeur peut comporter une réserve

La réalité

- Pour respecter les principes Trust nous avons dû revoir plusieurs contrôles
- Nous avons émis le rapport avec 18 jours de retard par rapport à l’échéancier prévu
- Le rapport de l’auditeur comportait une réserve

À retenir

- Ce sont les principes Trust qui dictent les résultats de l’audit et si le rapport comportera une réserve ou non
- Une gestion serrée du mandat est nécessaire (autant du côté de l’auditeur que de l’audité)
- Le rapport peut ne pas être publié; cela dépend des attentes de la haute direction et des utilisateurs


Fin

Leçons apprises

1. Comprendre les normes et se garder à jour
2. Gérer le dossier de façon *top-down* au lieu de *bottom-up*
3. Prévoir du temps de préparation et d'analyse de la situation sans créer d'attentes (de publier le rapport)
4. Prévoir que la préparation du premier rapport demande des efforts importants et une grande cohésion
5. Travailler en étroite collaboration avec les équipes qui doivent répondre à l'auditeur
6. Déterminer à l'avance les conditions pour lesquelles vous n'émettrez pas le rapport
7. Être capable de détecter les déficiences potentielles est une grande force
8. Même si l'étendue de l'audit ne couvre que les TI, l'émission de ce rapport est l'affaire de toute l'organisation

Si vous avez des questions additionnelles ou besoin d’un conseil :

denis.jolin@desjardins.com