www.pwc.fr

SOC 2 et 3 : renforcer la confiance et la transparence avec vos clients

Des standards qui permettent d'aller au-delà du contrôle interne relatif à l'élaboration des états financiers.

Découvrez les standards d'attestation SOC 2 et 3 : objectifs, avantages et tendances.

pwc

Construire un écosystème de confiance avec vos parties prenantes

Spécialisation, outsourcing, offshoring, réduction des coûts – telle est la réalité des entreprises aujourd'hui.
Que ce soit pour une entreprise faisant appel à un prestataire ou pour le prestataire lui-même, il est plus que jamais nécessaire de construire un écosystème de confiance avec l'ensemble des parties prenantes.

L'augmentation du « Software as a Service », « Platform as a Service » et autres modèles d'infrastructure basés sur le Cloud et permettant de stocker toujours plus de données, fait croître le marché de l'externalisation. L'une des conséquences est la nécessité d'obtenir une évaluation indépendante des contrôles en place chez les prestataires.

Connu également comme le « Statement on Standards for Attestation Engagements » SSAE 18, le « Service Organization Control » SOC 1 est conçu pour évaluer l'efficacité du contrôle interne des processus et des systèmes relatifs à l'élaboration des états financiers mais ne couvre pas des besoins plus larges, notamment en termes de contrôles de conformité et de tests opérationnels pour des entreprises faisant appel à des prestataires.

L'« American Institute of Certified Public Accountants » AICPA et le « Canadian Institute of Chartered Accountants » CICA ont compris le besoin de suivi des contrôles dans des situations différentes de celles impliquant directement le contrôle interne relatif à l'élaboration des états financiers. Dans ce but, ils ont créé deux standards d'attestation : SOC 2 et SOC 3.

SOC 2 et SOC 3 s'appuient sur les « Trust Services Categories » et les « Trust Services Criteria » comme cadre permettant l'évaluation des contrôles de conformité et opérationnels pertinents pour les entreprises faisant appel à des prestataires.

Les rapports SOC 2 et SOC 3 apportent aux entreprises la confiance et la transparence dont elles ont besoin concernant les contrôles de conformité et les contrôles opérationnels pour les fonctions qu'elles externalisent à des prestataires.

Quelles sont les différences fondamentales entre les rapports SOC 1, 2 et 3 ?

Contrôle interne relatif à l'élaboration des états financiers

SOC 1 – En remplacement des rapports « Statement on Auditing Standards » SAS 70, les rapports SOC 1 permettent d'émettre une opinion sur les contrôles en place chez un prestataire, en lien avec l'élaboration des états financiers des entreprises faisant appel à ce prestataire.

Contrôle interne allant au-delà des processus d'élaboration des états financiers

SOC 2 – Un rapport SOC 2 permet d'émettre une opinion sur les contrôles en place chez un prestataire, contrôles relatifs à la sécurité, la disponibilité, l'intégrité des traitements, la confidentialité et/ou la protection des données (appelés « Trust Services Categories »). Le format et la structure d'un rapport SOC 2 sont similaires à ceux d'un rapport SOC 1, bien que le contenu en diffère.

SOC 3 – Le rapport SOC 3 est très proche du rapport SOC 2. Les deux différences sont que l'information présentée dans un rapport SOC 3 est réduite (absence de description des contrôles, des procédures de tests et des résultats de ces tests) et sa distribution n'est pas restreinte, c'est-à-dire qu'il peut être partagé publiquement, sur Internet par exemple.

Comparaison des rapports SOC

Le tableau ci-dessous compare les objectifs et les avantages des trois rapports SOC.

Options possibles	Rapport du « Service Organization Control » N°1 (SOC 1 / SSAE 18)	Rapport du « Service Organization Control » N°2 (SOC 2)	Rapport du « Service Organization Control » N°3 (SOC 3)
Objectifs du rapport	Rapport sur le contrôle interne relatif à l'élaboration des états financiers	Rapport sur les contrôles concernant la sécurité, la disponibilité, l'intégrité des traitements, la confidentialité et/ou la protection des données	
Avantages	• Le rapport SOC 1 apporte de la transparence sur la description du système, les contrôles, les procédures de tests et leurs résultats • Son usage est restreint à l'entreprise faisant appel à des prestataires et à ses auditeurs	• Le rapport SOC 2 apporte de la transparence sur la description du système, les contrôles, les procédures de tests et leurs résultats • Son usage est restreint à l'entreprise faisant appel à des prestataires, à ses auditeurs et à d'autres tiers spécifiques ayant une connaissance du système	• La distribution générale du rapport permet des bénéfices en termes de marketing • Le rapport ne contient pas les résultats détaillés de tests des auditeurs.
Sections du rapport	**Section I** « Report of Independent Service Auditor » **Section II** « Management's assertion » **Section III** « Description of the Service Organization's system » **Section IV** Pour les rapports Type 2, « Description of tests and related results »		**Section I** « Report of Independent Service Auditor » **Section II** « Management's assertion » **Section III** « Description of scope, or boundaries of system »
Opinion apportée	• La correcte description du système du prestataire • La correcte conception des contrôles, afin de fournir la garantie que les objectifs de contrôles et les « Trust Services Criteria » sont applicables et bien atteints et que les contrôles ont été opérés efficacement • Pour les rapports Type 2, si les contrôles ont été opérés efficacement sur une période définie afin d'atteindre les objectifs de contrôles et les « Trust Services Criteria » applicables		• La bonne conception et mise en place des contrôles concernant les systèmes relatifs aux « Trust Services Categories » dans le périmètre du rapport.

Un rapport SOC peut être de type 1 (l'opinion couvre uniquement la conception des contrôles, à un moment précis) ou de type 2 (l'opinion couvre une période de temps définie afin de s'assurer de l'efficacité opérationnelle des contrôles dans la durée, c'est-à-dire de la bonne application ou execution).

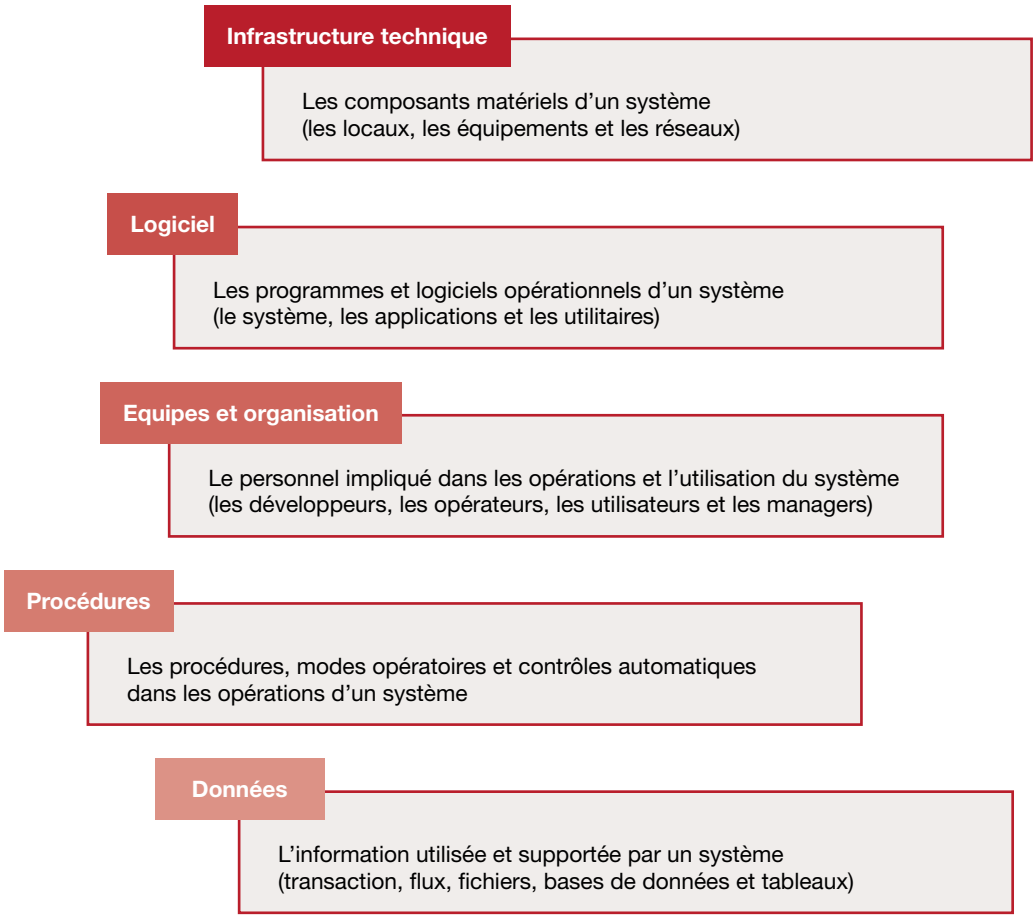
Quelles sont les « Trust Services Categories » ?

Il existe 5 « Trust Services Categories », chacune supportée par les « Trust Services Criteria » qui doivent être atteints afin que le système soit conçu de manière adéquate.

« Trust Services Categories »	Description	« Trust Services Criteria »
Sécurité	Le système est protégé contre les accès non autorisés (physiques et logiques).	Cette catégorie est centrée sur l'implémentation et la diffusion d'une politique de sécurité et des procédures associées. Elle inclut notamment : • Les exigences de sécurité liées aux utilisateurs autorisés ; • La communication et l'évaluation des risques ; • L'affectation des responsabilités de réalisation et de validation ; • La formation et la conformité avec les lois et réglementations ; • La gestion des failles de sécurité et autres incidents.
Disponibilité	Le système est disponible pour les opérations et son utilisation est effective.	Cette catégorie est centrée sur la définition des exigences de disponibilité pour les systèmes et sur les politiques et procédures requises. Elle inclut notamment : • L'implémentation des mesures qui préviennent ou réduisent les menaces ; • La gestion des exceptions concernant la disponibilité des systèmes ; • Les procédures qui permettent l'intégrité des données de sauvegarde d'informations et des systèmes maintenus pour supporter les politiques de sécurité.
Confidentialité	L'information identifiée comme confidentielle est protégée.	Cette catégorie est centrée sur la définition des exigences de confidentialité des données au travers des politiques et des procédures. Elle inclut notamment : • La compréhension des façons dont l'information confidentielle est accessible, utilisée et divulguée ; • Les procédures liées à la confidentialité des données en entrée, de leur traitement et des données en sortie, en accord avec les politiques ; • A la protection des informations confidentielles pendant les activités de gestion du changement.
Intégrité des traitements	Les traitements sont complets, exacts, opportuns et autorisés.	Cette catégorie est centrée sur la documentation et l'implémentation des contrôles afin de s'assurer que les traitements se déroulent comme prévu. Elle inclut notamment : • Les procédures de gestion des données, leur exhaustivité, leur exactitude, leur correcte mise à jour et l'autorisation des données en entrée, conformément aux politiques définies ; • Les procédures de gestion des exceptions en accord avec les politiques existantes. Note : des exigences supplémentaires s'appliquent pour les systèmes de e-commerce.
Protection des données ou « Privacy »	La donnée est collectée, utilisée, maintenue, divulguée et supprimée en conformité avec les engagements de la politique de protection des données et les critères définis par l'AICPA et le CICA.	Cette catégorie liée à la protection des données est la plus conséquente et exige la définition, la documentation et la communication (ainsi que la responsabilité associée) des politiques et procédures associées à la protection des données. L'organisation doit considérer et implémenter ces procédures en prenant en compte les éléments suivants : • La gestion des politiques et procédures liées à la gestion de données ; • La collecte, l'utilisation, la rétention et la divulgation des données ; • La divulgation de données à des tiers ; • Les incidents liés aux données et à la gestion des failles.

Composants du système du prestataire

SOC 2 et SOC 3 utilisent le même référentiel de contrôle basé sur les « Trust Services Categories » et les « Trust Services Criteria ».
Dans un rapport SOC 2 ou SOC 3, le management fournit une lettre d'affirmation qui est validée par l'auditeur et qui inclut les cinq composants suivants :



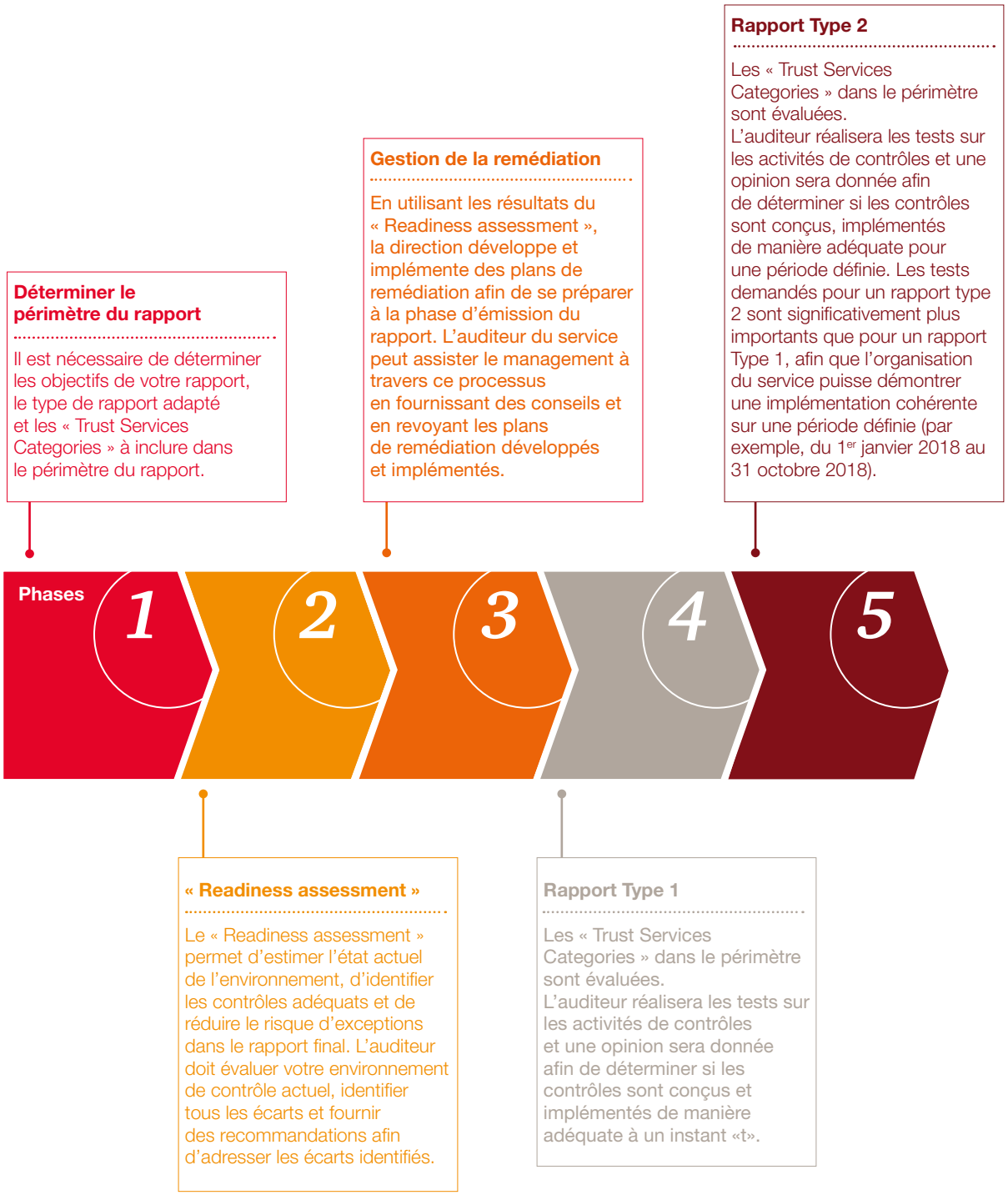
Définir le périmètre

Les rapports SOC 2 et SOC 3 disposent tous deux de « Trust Services Categories » et de « Trust Services Criteria ».
Les « Trust Services Categories » évaluées sont sélectionnées par le prestataire – c'est-à-dire qu'il peut choisir quelle « Trust Services Category » ou combinaison de « Trust Services Categories » est à inclure dans le périmètre de son rapport SOC 2 ou SOC 3.

Cette flexibilité crée un réel avantage : le prestataire peut évaluer de manière stratégique ses composants et cibler les « Trust Services Categories » ayant un intérêt majeur pour ses clients et prospects.
Il est cependant important de noter que pour chaque « Trust Services Category » incluse dans le périmètre, tous les « Trust Services Criteria » et contrôles associés doivent être adressés dans les rapports SOC 2 et SOC 3.

Comment se déroule un audit SOC 2 et SOC 3 ?

Nous pouvons aider dans une ou l'ensemble des phases mentionnées ci-dessous, qui se déroulent habituellement comme suit :



Observations et tendances

La sécurité d'abord !

Aujourd'hui, la « Trust Services Category » la plus demandée est celle liée à la Sécurité, suivie par celle liée à la Disponibilité. La plupart des entreprises optent pour une ou deux « Trust Services Categories » pour leur premier rapport SOC, à savoir Sécurité et une autre « Trust Services Category », si besoin.

Cette approche leur permet de se concentrer sur les critères à atteindre pour chaque « Trust Services Category » choisie, tout en continuant de renforcer leur maturité Business sur d'autres domaines afin de mieux se positionner et étendre le périmètre de leurs prochains rapports, si nécessaire. Au fil des années, les prestataires peuvent envisager d'ajouter des processus, des locaux ou des « Trust Services Categories » dans le périmètre de leur rapport. Cette démarche est généralement basée sur des demandes explicites de leurs clients, sur des changements de risques métier ou de produits et services.

Rapports SOC 2 et 3 simultanés

Occasionnellement, les prestataires demandent l'émission de rapports SOC 2 et SOC 3 de façon simultanée sur le même environnement. Ils peuvent ainsi fournir à leurs clients le niveau de détail qu'ils demandent à travers le rapport SOC 2 tout en utilisant le rapport SOC 3 dans un but marketing : cela les aide à se différencier de leurs concurrents.

> ***Notre expérience a révélé que les entreprises sous-estiment souvent l'effort et la charge de travail nécessaires à l'émission des rapports.***

Que faire si votre rapport SOC 2 ne couvre pas toutes les préoccupations de vos clients ?

Si le référentiel de contrôle lié aux « Trust Services Categories » retenues dans votre rapport SOC 2 ne couvre pas l'intégralité des sujets de préoccupation, vous pouvez décider d'inclure dans votre rapport des critères additionnels (par exemple, concernant la gestion du cycle de développement ou la conformité à certaines exigences contractuelles). Les rapports SOC 2+ permettent d'ajouter des critères complémentaires qui peuvent vous permettre de vous démarquer de vos concurrents tout en réduisant le nombre d'audits sur place.

Vos contacts

Anne-Christine Marie
Associée Gestion des risques liés aux tiers
01 56 57 13 42
anne-christine.marie@pwc.com

Pierre-Olivier Duranton
Associé Gestion des risques liés aux tiers
01 56 57 73 53
pierre-olivier.duranton@pwc.com

Fabrice Garnier de Labareyre
Associé Cybersécurité
01 56 57 58 18
fabrice.garnier.de.labareyre@pwc.com

Florian Abegg
Directeur Gestion des risques liés aux tiers
01 56 57 70 58
florian.abegg@pwc.com

Pour le secteur des services financiers :

Romain Camus
Associé Gestion des risques liés aux tiers
Banque et Asset Management
01 56 57 87 83
romain.camus@pwc.com

Karine Pariente
Associée Gestion des risques liés aux tiers
Compagnies d'Assurance et Immobilier
01 56 57 70 09
karine.pariente@pwc.com