Article

Mythes courants sur les rapports de contrôle des prestataires de services (rapports SOC)

Deepa Seshadri, CISA, CISM, est directeur principal chez un des "Big Four" et a 15 ans d'expérience en tant que spécialiste des contrôles internes. Elle a participé à des évaluations de tiers, des revues des normes SAS 70/SSAE 16/ISAE 3402, des revues de sécurité et d'infrastructures, des revues des contrôles généraux informatiques et des revues d'applications dans divers environnements techniques. Elle a également effectué plusieurs revues de développement offshore, notamment dans les domaines de la fabrication, des logiciels et des services bancaires et financiers.

Dans les environnements dynamiques actuels, les organisations sont confrontées à de nombreux défis en matière de respect des différentes normes et de mise en conformité. Elles doivent fournir à leurs clients des certificats, des avis et des rapports à des fins diverses. Néanmoins, il est souvent difficile pour ces organisations de déterminer avec certitude la pertinence d'un certificat ou avis pouvant constituer une assurance pour leurs clients.

Cet article présente les rapports disponibles sur les contrôles des prestataires de services (SOC). Cet article vise également à mettre en lumière les principales erreurs ou abus de langage liés à l'utilisation de ces rapports SOC, ainsi que des conseils importants dont les organisations doivent se souvenir pour s'assurer que leurs investissements dans ce type d'activités portent leurs fruits et profitent réellement à leurs clients.

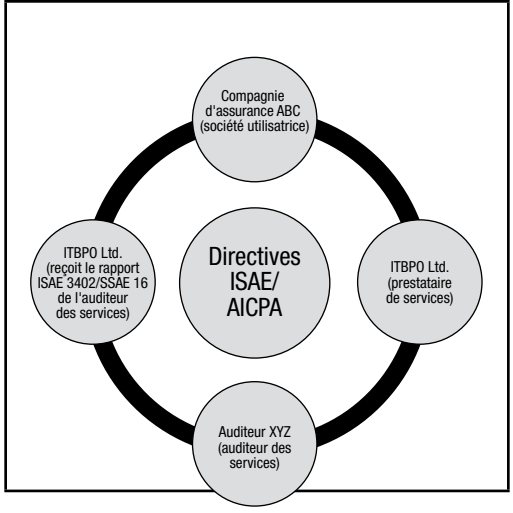
PROCESSUS DE CRÉATION D'UN RAPPORT SOC[1]

En décembre 2009, l'IAASB (*International Auditing and Assurance Standards Board*) a publié une nouvelle norme internationale sur les missions d'assurance, l'ISAE 3402, relative aux contrôles réalisés par les prestataires de services. Par la suite, l'AICPA (*American Institute of Certified Public Accountants*) a modifié la norme SAS 70 (*Statement on Auditing Standards*) qui concerne la production de rapports d'assurance sur les contrôles mis en œuvre dans les sociétés prestataires de services, donnant ainsi naissance à la norme SSAE 16 (*Statement on Standards for Attestation Engagements*).

L'exemple fictif suivant explique le fonctionnement du processus défini par les normes ISAE 3402/SSAE 16. La compagnie d'assurance ABC sous-traite certaines tâches de traitement des déclarations au prestataire de services ITBPO Ltd. Selon la terminologie ISAE 3402/SSAE 16, la compagnie d'assurance ABC est l'entité utilisatrice et ITBPO Ltd. la société de services. Pour s'assurer que la société de services traite correctement les déclarations et applique les contrôles internes appropriés, l'entité utilisatrice nomme un expert-comptable agréé ou un auditeur des services (Auditeur XYZ) pour examiner les contrôles du prestataire et donner son avis. Le prestataire de services doit démontrer qu'il répond aux exigences de l'entité utilisatrice et obtenir une évaluation objective de l'efficacité des contrôles sur les opérations, la conformité et les rapports financiers. L'expert-comptable s'appuie sur les différents rapports SOC encadrés par la norme ISAE 3402 ou SSAE 16 (SOC 1, SOC 2 et SOC 3) pour examiner les contrôles et aider la direction à appréhender les facteurs de risque inhérents. À partir des directives de l'IAASB/AICPA, l'auditeur des services réalise la mission et fournit le rapport à ITBPO Ltd., qui, à son tour, transmet le rapport à la compagnie d'assurance ABC.

L'approche globale est décrite **figure 1**.

Figure 1—Approche relative aux rapports relatifs aux prestataires de services



Les prestataires de services peuvent fournir ces rapports à différentes entités utilisatrices afin de les rassurer sur le fonctionnement des contrôles internes. Pour obtenir ce rapport SOC 1, un prestataire peut nommer un auditeur des services indépendant qui réalisera l'audit. Un rapport SOC 1 est une assurance sur les contrôles sous-jacents aux contrôles internes des rapports financiers. Le prestataire peut ensuite le transmettre aux entités utilisatrices et à leurs auditeurs sur demande ou si elle le juge nécessaire.

L'AICPA propose également deux autres rapports : SOC 2 et SOC 3. Les rapports SOC 2 et SOC 3 évaluent les contrôles autres que les contrôles internes des rapports financiers. L'une des différences majeures entre ces deux rapports est que le SOC 3 constitue un rapport d'ordre général pouvant s'adresser à quiconque, tandis que le SOC 2 est destiné aux utilisateurs spécifiés dans le rapport.

SOC 1 : MYTHES ET RÉALITÉ

Les prestataires de services adoptent fréquemment les rapports SOC 1 (ISAE 3402/SSAE 16 de type I et de type II) pour de mauvaises raisons, les rapports SSAE 16 étant anciennement connus sous le nom de rapports SAS 70. Voici quelques-unes des erreurs les plus courantes concernant leur adoption :

1. **Ces rapports sont des certifications.** Une fois la mission terminée, les organisations déclarent à leurs clients et aux parties prenantes qu'elles sont certifiées SOC 1 ou SSAE 16.

   En réalité : Les directives de l'IAASB/AICPA indiquent clairement que les rapports ISAE 3402/SSAE 16 ne sont pas des certifications. Elles précisent que la distribution de ces rapports est restreinte et que leur utilisation est exclusivement destinée au prestataire de services, à l'entité utilisatrice et aux auditeurs de cette dernière.
2. **Ces rapports peuvent généralement être transmis aux clients potentiels et utilisés comme documents marketing.** Les organisations transmettent ou envisagent de transmettre les rapports de type I et de type II à leurs clients potentiels, sans tenir compte des restrictions d'utilisation.

   En réalité : Les rapports SOC sont publiés par le prestataire de services dans un but bien précis. Ils sont destinés à un public clairement défini. La diffusion de ces rapports est généralement limitée et il existe des restrictions d'utilisation spécifiques.
3. **Tous les domaines d'exploitation peuvent être inclus dans les rapports SOC 1.** Les organisations étendent sans réfléchir ces contrôles aux domaines opérationnels, marketing et réglementaires n'ayant aucune incidence directe ou indirecte sur les rapports financiers.

   En réalité : Les directives de l'IAASB/AICPA précisent que le rapport SOC 1 s'applique uniquement aux contrôles internes des rapports financiers. Si les organisations souhaitent intégrer d'autres domaines, tels que la confidentialité et le respect de la vie privée, elles doivent adopter les rapports SOC 2/SOC 3. La différence majeure réside dans le fait que les rapports SOC 1 sont exclusivement destinés aux contrôles internes des rapports financiers, tandis que les rapports SOC 2/SOC 3 couvrent des domaines relatifs à la sécurité, la confidentialité, la disponibilité et la vie privée.
4. **Après l'obtention du rapport, l'entité utilisatrice n'est pas tenue de vérifier les contrôles.** Très souvent, les parties prenantes s'appuient sur les rapports SOC, consultent de façon isolée les contrôles qui sont définis dans le rapport sans prendre en compte ceux qui sont réalisés au niveau de l'entité utilisatrice.

   En réalité : Lors de l'évaluation des contrôles effectués par le prestataire de services, il est essentiel de prendre également en compte ceux effectués par l'entité utilisatrice.
5. **Il est possible de rendre conforme le logiciel applicatif aux exigences de la norme SSAE 16.** Lorsque les fournisseurs de logiciels développent une application dédiée aux rapports financiers, ils souhaitent généralement qu'elle soit conforme aux exigences de la norme SSAE 16.

   En réalité : Les rapports SOC 1 constituent généralement une garantie sur les contrôles internes des rapports financiers et non une évaluation des produits.
6. **Le travail effectué par un auditeur interne ne peut pas être utilisé pour les missions encadrées par la norme SSAE 16.** Le travail de l'auditeur interne ne s'intègre pas dans les évaluations réalisées dans le cadre de la norme SSAE 16.

   En réalité : Le travail d'un auditeur interne peut être utilisé dans une mission encadrée par la norme SSAE 16 et la décision de le prendre en compte relève de l'auditeur des services.
7. **L'auditeur des services doit vérifier l'exactitude de la section relative aux « autres informations fournies par prestataire de services ».** Les prestataires de services fournissent une quantité importante d'informations (par ex., le plan de continuité des activités) dans cette section. Les organisations partent de l'hypothèse selon laquelle l'exactitude de ces informations n'est pas forcément vérifiée par l'auditeur des services.

Cet article vous intéresse ?

- Lisez le *guide d'utilisation du SOC 2*.
  www.isaca.org/soc2
- Consultez le centre de connaissances pour obtenir plus d'informations, travailler en collaboration et entamer des discussions sur la gestion des services.
  www.isaca.org/knowledgecenter

En réalité : Le prestataire de services a l'obligation de vérifier que les informations fournies sont exactes ; toutefois, l'auditeur des services ne donne pas son avis sur cette section.

8. **L'auditeur des services ne teste pas l'efficacité des contrôles au niveau de l'entité.** Les contrôles inhérents à l'entité décrits par le prestataire de services sont exploités par l'auditeur des services, mais aucun test n'est effectué.

   En réalité : Les auditeurs des services donnent leur avis sur les contrôles au niveau de l'entité, notamment sur l'environnement de contrôle, l'évaluation des risques, l'information et la communication, ainsi que sur la surveillance.

9. **La période de test des contrôles doit être de six mois.** Les organisations évitent de réaliser des rapports SOC 1 si les contrôles ont été récemment conçus, pensant que les rapports SOC 1 ne sont pas valables.

   En réalité : Dans certaines circonstances, les rapports peuvent être publiés pour une période inférieure à six mois, auquel cas l'auditeur des services indique les restrictions applicables dans la section 1 du rapport.

CONCLUSION

Les normes SSAE 16 de l'AICPA et ISAE 3402 de l'IAASB définissent l'objectif des rapports SOC 1 : ils sont destinés à fournir une assurance sur les contrôles sous-jacents aux contrôles internes des rapports financiers. C'est pourquoi les organisations doivent s'évertuer à comprendre la finalité d'un rapport SOC 1 tout en définissant précisément le périmètre des processus à couvrir. Ce rapport peut s'avérer particulièrement utile aux entités utilisatrices qui souhaitent comprendre les contrôles ayant une incidence sur les opérations financières et les contrôles informatiques inhérents qui sont effectués par le prestataire de services, notamment lorsqu'elles font appel à plusieurs prestataires de services.