

Audits de TI : informatique en nuage et services SaaS

Tommie W. Singleton, Ph. D., CISA, CITP, CMA, CPA

La loi de Moore, qui s'applique depuis des décennies et ne semble pas encore avoir atteint ses limites, a donné lieu à nombre de nouvelles technologies et, partant, à de nouveaux défis pour les auditeurs. Au cours des récents mois, l'informatique en nuage (ou infonuagique) et les services SaaS (pour « Software as a Service ») ont été à l'avant-garde des technologies de l'information. Les auditeurs de TI doivent par conséquent obtenir une compréhension de ces technologies, établir une approche afin d'identifier les principaux risques et planifier des audits efficaces des technologies pour tenir compte de ces risques. En ce qui a trait à l'informatique en nuage, l'approche fondée sur les risques est cependant compliquée par le fait que toutes les technologies et tous les contrôles sont hébergés à l'extérieur de l'entité auditée^{1,2,3}.

La clé d'un audit TI visant une informatique en nuage et des services SaaS réside dans le choix d'un référentiel pour encadrer les différents services et permettre d'évaluer efficacement les risques liés à ces technologies. Lorsque l'évaluation des risques est appropriée, l'audit des TI devient le prolongement naturel de l'audit fondé sur les risques identifiés, en particulier lorsque les contrôles ne réduisent pas suffisamment les risques. L'approche fondée sur les risques est aujourd'hui la plus répandue pour divers types d'audits.

Les éléments de l'informatique en nuage

L'informatique en nuage a fait l'objet d'un grand nombre d'études, tout comme les services SaaS et les centres de données. Ces technologies sont cependant imbriquées les unes dans les autres et proposées comme un ensemble de services que l'on désigne souvent par « informatique en nuage ». Il existe un référentiel simple concernant l'informatique en nuage qui devrait aider les auditeurs de TI pour l'évaluation des risques. L'informatique en nuage repose en effet sur des éléments matériels ou services IaaS (pour « Infrastructure as a Service ») et des éléments logiciels ou services SaaS (pour « Software as a Service »), qui présentent de grandes analogies avec la façon dont nous concevons l'ensemble des technologies internes d'une entité.

Informatique en nuage : services IaaS

Les services IaaS remplacent ou complètent l'infrastructure interne. La direction d'une entité appuie habituellement sa décision de passer à l'IaaS (externalisation d'une partie de son infrastructure) et son choix de fournisseur de tels services principalement sur des facteurs liés à l'efficacité. Par exemple, il faut un « nombre X d'heures » par année à un employé équivalent temps plein (ETP) pour gérer environ 70 serveurs. Si l'entité dispose d'un parc de serveurs, elle peut externaliser ces tâches vers un centre de données efficace et réduire les coûts substantiellement. Dans ce cas, lorsque l'entité doit mettre à niveau ou faire l'acquisition de logiciels, le facteur coût de l'infrastructure devient négligeable si le choix du

¹ Raval, Vasant, « Risk Landscape of Cloud Computing », *ISACA Journal*, ISACA, États-Unis, vol. 1, 2010.

² Ross, Steve, « Cloudy Daze », *ISACA Journal*, ISACA, États-Unis, vol. 1, 2010.

³ Gadia, Sailesh, « Cloud Computing: An Auditor's Perspective », *ISACA Journal*, ISACA, États-Unis, vol. 6, 2009.

fournisseur de services IaaS a été suffisamment éclairé et que l'infrastructure de l'entité nécessite peu de modifications, voire aucune.

Il faut aussi considérer le facteur comptabilité. Les coûts de l'infrastructure sont habituellement importants et, selon les principes comptables généralement reconnus (PCGR), ils sont traités comme une dépense en immobilisations. Cependant, si l'infrastructure est externalisée, la charge associée aux services IaaS devient habituellement une charge d'exploitation. Aux États-Unis, elle donne même lieu à un avantage fiscal qui permet de réduire les impôts sur le résultat.

Les critères dont la direction doit essentiellement tenir compte lorsqu'elle choisit son fournisseur de services IaaS sont donc la souplesse d'utilisation (y compris l'extensibilité) et la disponibilité ainsi que la sécurité physique et virtuelle.

Voici certaines catégories de services IaaS :

- Connectivité
- Services de réseau et gestion
- Services de calcul et gestion
- Stockage de données
- Sécurité

Par connectivité, on entend évidemment l'accès fiable à Internet et la connectivité aux systèmes et aux technologies connexes (par exemple, le stockage des données pour les serveurs d'application). Des exemples de risques liés à la connectivité sont la disponibilité et le temps d'indisponibilité ainsi que la vitesse d'accès⁴. Pour une entité moyenne, le temps d'arrêt correspond à une journée par année.

Les services de réseau et gestion englobent autant les ressources liées au réseau que la gestion et la surveillance du réseau, ainsi que l'accès efficace au réseau en tenant compte de facteurs comme l'équilibrage du trafic. Les risques liés aux services de réseau et à la gestion ont trait à l'extensibilité des nouvelles technologies ou au rehaussement du niveau des opérations, à la disponibilité, à la sécurisation des transmissions et à l'accessibilité (équilibrage du trafic, par exemple).

Les services de calcul et gestion comprennent l'accès aux ressources appropriées comme le cœur des processeurs, les processeurs, la mémoire et la gestion du système d'exploitation. Les risques liés à ces services ont trait à la disponibilité (notamment les pannes de système) et à l'extensibilité.

Les centres de données ont connu une forte croissance au cours des dernières années et les services offerts sont de plus en plus perfectionnés. Les risques liés au stockage de données ont trait notamment à la sécurité des données, à la récupération des données, à l'accessibilité et à l'extensivité. Les questions liées à la sécurité et à la récupération des données sont particulièrement importantes. La direction doit en effet s'assurer que l'élément stockage de données des services IaaS peut offrir un niveau approprié de

⁴ Chaque audit de TI a son propre contexte (audit financier, interne, audit TI spécial) et il a aussi ses objectifs de base. Un audit de TI en particulier portera donc sur tous ces facteurs de risque pour divers aspects de l'informatique en nuage et déterminera s'ils sont applicables et pertinents.

sécurité physique et logique et que la méthode de récupération des données est appropriée et permet une reprise rapide des activités si le centre de données subit un sinistre.

Les questions de sécurité sont plus ou moins omniprésentes pour les services IaaS et concernent la sécurité physique, en particulier le stockage des données, et la sécurité logique. Elles portent plus précisément sur les intrusions malveillantes par des utilisateurs et des employés non autorisés du fournisseur des services IaaS. En fait, le risque lié aux employés du fournisseur est un risque élevé pour l'entité utilisatrice et il doit être éliminé, sinon atténué, au moyen de contrôles adéquats par le fournisseur de services.

Les risques sont toujours déterminés par rapport au contexte dans lequel évolue l'entité, par exemple : le secteur d'activité, ses processus propres, la situation économique et d'autres circonstances propres à l'entité à ce moment. Parmi les autres facteurs de risque figurent la propriété, les assurances, la gestion de projets et l'information sur la performance.

Un rapport d'audit de type II selon SAS 70 peut permettre de découvrir les contrôles d'atténuation des risques mis en place. Si le fournisseur de services IaaS en produit un, l'auditeur de TI devrait le lire afin de déterminer quel type d'assurance il peut obtenir pour les risques spécifiques identifiés. Les contrôles mis en place par le fournisseur de services comprennent les meilleures pratiques en matière de sécurité, de soutien (p. ex., IT Infrastructure Library [ITIL] v3) et de reprise des activités.

Informatique en nuage : services SaaS

Les principaux critères de décision quant aux services SaaS ou au choix d'un fournisseur en particulier sont la complexité de l'environnement, la nécessité d'acheter des éléments ou des modules de plus petite taille, la compatibilité avec les systèmes et les technologies en place (y compris la plate-forme de programmation), la facilité d'acquisition et d'intégration, la gestion du projet, l'extensibilité de l'infrastructure et la facturation ou les coûts (mesure).

Voici une façon, parmi d'autres, de détailler les services SaaS :

- Modélisation des processus
- Évaluation et analyse
- Exécution des processus

La modélisation des processus a trait à la nécessité de faire correspondre entre eux le déroulement des activités/les processus, les applications et les données, la structure organisationnelle et l'intégration des systèmes existants. L'évaluation et l'analyse comprennent la comptabilisation des coûts des processus, les tableaux de bord, les accords sur les niveaux de service ainsi que l'entreposage et l'optimisation des processus. L'exécution des processus comprend les éléments suivants : le contrôle du déroulement des activités, l'intégration des applications (intégration d'application d'entreprise [EAI]), l'orchestration des services (architecture orientée services), la constitution des bases de données ou leur conversion, ainsi que la surveillance des activités. Il faut aussi tenir compte de la gestion des documents et du contenu, de

la collaboration, de la gestion et de l'administration des systèmes ainsi que de divers autres aspects de la gestion des SaaS.

Les risques sont liés aux aspects ci-dessus et ont trait notamment à l'inadéquation des processus et des applications, à la connectivité insuffisante entre les applications et les données, à l'échec de l'intégration avec les systèmes en place ainsi qu'à la surveillance inadéquate des processus et des incidents liés aux services SaaS. L'un des principaux objectifs de l'audit concerne les accords sur les niveaux de service. Il existe aussi un risque lié au contrôle des coûts et aux estimations puisque le changement pourrait en définitive représenter un coût supplémentaire pour l'entreprise. L'aspect facturation/mesure des services SaaS est un exemple de contrôle des coûts qui peut constituer un facteur de risque.

Cadre de certification TI

Le cadre de certification TI de l'ISACA (IT Assurance Framework™ ou ITAF™) contient des indications (section 3630.6) sur l'impartition et les activités confiées à des tiers (voir la **figure 1**) qui renvoient également à d'autres référentiels comme le COBIT® (PO4, PO7, PO8, PO9, AI2 et AI5) et les *IT Audit and Assurance Guidelines* (autrefois *IS Audit Guidelines*) G4, G18, G32 et G37 de l'ISACA. Ces documents fournissent une aide technique utile pour l'exécution d'un audit de TI en informatique en nuage.

Figure 1 : Types de rapports fondés sur les besoins des utilisateurs

<p>Section 3630.6 Activités externalisées et activités de fournisseurs TI tiers (en anglais)</p> <p>Cette section fournit de l'information sur les différentes solutions d'impartition (externalisation, internalisation, délocalisation, gestion des installations, etc.), sur les activités TI susceptibles d'être imparties (exploitation, services de dépannage informatique, maintenance, soutien logiciel des systèmes et des applications, etc.) et sur les questions concernant ces modèles d'impartition dont le professionnel en certification des TI doit tenir compte.</p> <p>Les indications font aussi état des risques associés aux divers modèles d'impartition et fournit de l'information sur la façon dont la direction peut réduire ou atténuer ces risques.</p> <p>La section contient en outre des conseils utiles au sujet de la sous-traitance, de la réduction des risques liés à l'impartition de services, des recours juridiques et autres mesures de protection.</p>	<ul style="list-style-type: none"> • G4 Impartition des activités liées aux SI à d'autres organisations • G18 Gouvernance des TI • G32 Plan de continuité des activités — examen du point de vue des TI • G37 Processus de gestion des configurations • COBIT : <ul style="list-style-type: none"> ○ P04 Définition des processus, de l'organisation et des relations en TI ○ P07 Gestion des ressources humaines en TI ○ P08 Gestion de la qualité ○ P09 Évaluation et gestion des risques liés aux TI ○ AI2 Acquisition et mise à niveau des logiciels d'application ○ AI5 Acquisition de ressources en TI
<p>Source : ISACA, ITAF : <i>A Professional Practices Framework for IT Assurance</i>, États-Unis, 2008</p>	

Lorsque l'entité a confié des services à un tiers fournisseur de services, l'audit direct de ce fournisseur de services n'est pas toujours pratique, voire possible. L'ITAF fournit également une liste des documents susceptibles de fournir des informations pertinentes concernant l'audit de services (se reporter à la **figure 2**).

Figure 2 : Lignes directrices de l'ITAF pour l'audit d'activités liées aux TI fournies par des tiers

Besoins des utilisateurs du rapport	Services de consultation	Procédures d'attestation	Procédures convenues	SAS 703 S-59704	Services Trust, SysTrust et Web Trust
Le rapport fournit :	Aucune assurance	Une assurance	Aucune assurance	Une assurance	Une assurance par rapport à des critères prédéfinis
Le rapport est :	Réservé à un public prédéfini	Destiné à des fins de distribution générale	Réservé à ceux qui ont convenu des procédures	Réservé aux clients et à leurs auditeurs	Destiné à des fins de distribution générale
Le rapport contient :	Des informations détaillées	Des informations limitées	Des procédures spécifiques et des constatations factuelles	Des informations détaillées	Des informations précises qui peuvent être résumées ou détaillées

Source : ISACA, *ITAF : A Professional Practices Framework for IT Assurance*, États-Unis, 2008

Conclusion

L'audit de solutions d'informatique en nuage ressemble à l'audit de n'importe quelle nouvelle TI, c'est-à-dire que l'auditeur doit comprendre la TI, identifier les risques, évaluer les contrôles d'atténuation des risques et auditer les éléments à risque. L'acquisition de compréhension de la nouvelle technologie et l'évaluation des risques qui lui sont associés peuvent être étayées par un référentiel solide sur les TI et les risques et, par conséquent, aider l'auditeur de TI à effectuer une évaluation efficace des risques. Le référentiel de services IaaS/SaaS décrit dans le présent article vise à aider les auditeurs de TI à s'acquitter de leurs tâches relativement à l'informatique en nuage.

Tommie W. Singleton, Ph. D., CISA, CITP, CMA, CPA

est professeur agrégé en systèmes d'information (SI) à l'Université de l'Alabama à Birmingham (États-Unis). Il est titulaire d'une bourse de recherche Marshall dans le domaine des SI et il est aussi directeur du programme de juricomptabilité. Avant d'obtenir son doctorat en comptabilité à l'Université du Mississippi (États-Unis) en 1995, M. Singleton a été président d'un petit fournisseur à valeur ajoutée de systèmes d'information spécialisés en comptabilité et destinés aux micro-ordinateurs. M. Singleton est aussi chercheur invité dans les domaines de l'audit des TI et de la juricomptabilité à Carr Riggs Ingram, un grand cabinet régional d'expertise comptable du sud-est des États-Unis. En 1999, l'Alabama Society of CPAs a décerné à M. Singleton un prix pour son utilisation innovatrice de la technologie en 1998-1999 (Innovative User of Technology Award). Tommie Singleton est le porte-parole de l'ISACA auprès de l'Université de l'Alabama à Birmingham. Ses articles sur la fraude, les TI/SI, l'audit des TI et la gouvernance des TI ont été publiés dans de nombreuses revues, notamment l'*ISACA Journal*.

L'ISACA Journal (anciennement l'Information Systems Control Journal) est publié par l'ISACA, organisme sans but lucratif créé dans l'intérêt du public en 1969. Les membres de l'association, organisme bénévole au service des professionnels de la gouvernance des TI, reçoivent un abonnement annuel à l'ISACA Journal.

Les opinions exprimées dans l'ISACA Journal sont celles des auteurs et des annonceurs. Elles peuvent être différentes des politiques et des énoncés de position officiels de l'ISACA ou de l'IT Governance Institute et de leurs comités, ainsi que des opinions cautionnées par les auteurs, les employeurs ou les rédacteurs en chef de la présente publication. L'ISACA Journal ne garantit pas l'originalité du contenu des articles publiés par les auteurs.

Source : « IT Audits of Cloud and SaaS », par Tommie W. Singleton, Ph. D. , CISA, CITP, CMA, CPA, (ISACA Journal, volume 3) © 2010 ISACA®. Tous droits réservés. Traduction de l'anglais au français autorisée par l'ISACA. CGA-Canada assume l'entière responsabilité de l'exactitude et de la fidélité de la traduction.