Grant Thornton

L'instinct de la croissance™

Option Finance
04/01/2019

Par Florian Abegg,
directeur, Grant Thornton

Externalisation : les normes ISAE, un gage de confiance et une exigence de méthodologie

L'entreprise qui sous-traite demeure – quels que soient les engagements de résultats de ses sous-traitants et leur couverture en assurance – responsable en première ligne, tant vis-à-vis de ses distributeurs et clients, de ses collaborateurs, que des régulateurs de tout ordre.

Cette responsabilité, qui engage sa réputation, peut être mise à mal comme le témoigne la récente condamnation publique par la CNIL d'une entreprise qui n'a pas suffisamment protégé les données des visiteurs de son site Internet, dont le développement avait été confié à un prestataire.

Sur un marché particulièrement concurrentiel, comme celui de la paie, les acteurs qui peuvent communiquer des rapports sur leurs contrôles ont ainsi clairement un avantage compétitif. Toutefois, du côté des prestataires, il est souvent fastidieux de répondre à la fois aux questions relatives aux risques dans les appels d'offres et aux demandes d'audit des clients existants qui se multiplient. Enfin, les processus d'externalisation en cascade rendent de plus en plus complexes et difficiles l'accès à l'information sur toute la chaîne d'externalisation, et cela est d'autant plus vrai en cas d'absence de rapports sur le contrôle interne des différents prestataires.

Illustration de cette prise de conscience des acteurs – notamment soumis à des régulations liées à leurs activités ou qui externalisent la gestion de données sensibles –, les rapports ISAE («International Standard on Assurance Engagements») deviennent la norme. Ils sont même devenus un «deal breaker» car la sécurité des données est pour eux une priorité absolue. L'auditeur indépendant, grâce à des tests portant sur la conception et sur l'efficacité opérationnelle des contrôles peut accompagner un prestataire pour l'émission d'un rapport conforme à la norme. Déclinée en deux sous-ensembles, elle permet d'attester le contrôle interne relatif au reporting des états financiers (ISAE 3402) ainsi qu'aux autres informations (ISAE 3000). Ce dernier peut permettre à un prestataire de démontrer sa conformité au RGPD, de vérifier que les engagements contractuels sont tenus, ou à faire attester d'informations relatives au RSE, pour une externalisation socialement responsable.

Clauses d'audit, contrôles et pilotage adaptés au périmètre du rapport sont les priorités d'un déploiement réussi

Bien trop souvent, les entreprises n'exercent pas les clauses d'audit de leurs contrats de prestations, ou alors uniquement en cas de défaillance avérée. Or, une surveillance périodique par exemple par un audit sur les contrats les plus importants, peut permettre d'obtenir une assurance raisonnable sur le degré de maîtrise des opérations. A ce titre, il est important de noter que certaines entreprises qui proposent des souscriptions uniquement en ligne pour des services de type SaaS ou Cloud et ne laissent pas ou peu de marge de manœuvre pour négocier le contenu du contrat y compris la clause d'audit.

Les contrôles dans le périmètre du rapport doivent être définis. Cela est plus ou moins complexe notamment en fonction du niveau d'homogénéité du contrôle interne au sein de l'organisation. Cela implique d'identifier le «dénominateur commun» des contrôles en place, si l'organisation souhaite un rapport à diffusion non limitée. Dans certains cas, un rapport ISAE dédié à un client sera préférable, pour limiter l'effort et/ou le risque de déviations. Une des vertus de la démarche ISAE est qu'elle permet de mieux définir le périmètre de responsabilité en termes de contrôle interne entre le prestataire, ses clients et potentiellement les prestataires de second rang. L'objectif étant in fine d'émettre un rapport non qualifié avec le minimum de déviations, l'audit à blanc est souvent nécessaire en particulier si aucun rapport n'a jamais été émis par le passé. Enfin, le pilotage du dispositif doit toujours être adapté, et proportionné aux risques. Sous réserve que l'entreprise ait bien pu conserver les compétences lui permettant de maintenir une appréciation et une gestion des risques afférents aux activités concernées, le suivi de la bonne mise en œuvre du contrat et les informations déclaratives du prestataire peuvent suffire dans certains cas. Cependant, le marché de l'externalisation étant en forte croissance, notamment tiré par les technologies comme le Cloud, l'automatisation des processus par la robotique (RPA), il est probable que dans les années à venir, le lien de dépendance et l'impact potentiel, en moyenne, se renforce. ■