

# >> Gestion des risques du SI par une approche holistique

**Christine LABARRE, Manager**

La gestion du risque n'est pas une activité nouvelle pour beaucoup d'organisations. Elles ont d'ailleurs appris depuis longtemps déjà à s'organiser pour maîtriser cette menace pour la création de valeur, en particulier dans les secteurs de la banque et de l'assurance.

En dépit de leur niveau de maturité important dans ce domaine, de nombreuses entreprises ont cantonné, au sein de la DSI, la gestion des risques spécifiques inhérents aux systèmes d'information, en raison de la complexité des décisions à mettre en œuvre.

Cependant, la croissance des contraintes réglementaires, le lien de plus en plus fort entre les métiers et les systèmes d'information, et l'exposition de leurs activités critiques aux risques SI amènent de plus en plus d'entreprises à adopter une approche holistique<sup>(1)</sup> permettant d'optimiser la position de l'entreprise face à son seuil de tolérance au risque.

## >> Les vulnérabilités du SI

L'information représente un actif majeur de l'entreprise au même titre que les autres actifs liés au système de production tels que les actifs physiques, sociaux, humains ou financiers. Elle acquiert encore de la valeur quand elle aide les métiers à répondre aux enjeux stratégiques de l'entreprise.

Entre les risques liés à l'activité et les risques technologiques, les causes possibles de défaillance sont nombreuses et le périmètre des risques du système d'information est étendu. Cependant, la prise en compte de ces risques est encore souvent gérée en silos (les risques opérationnels au niveau métier, les risques projets, la sécurité, la conformité, la gouvernance,...) et l'absence de critères de mesure communs et homogènes entraîne des disparités dans la priorisation des mesures correctives.

La mise en œuvre de la gestion de la sécurité du SI est un pré-requis à la gestion des risques SI. Les grandes orientations de sécurité sont définies à partir des enjeux et besoins métiers, et fondées sur des analyses des risques encourus par les différentes entités de l'entreprise. La valorisation de ces risques, comparée aux coûts des mesures de protection associées permet une optimisation des moyens consacrés à la sécurité.

Mais la gestion des risques du système d'information ne peut être bénéfique à terme que si elle répond aux attentes des métiers et est conforme à la position globale de l'entreprise.

Ainsi, les métiers doivent être responsabilisés sur le bon déroulement de leurs processus. Cette responsabilisation englobe les systèmes d'information sous-jacents et particulièrement le respect de la protection des données et la sécurité de l'information. Ils doivent comprendre qu'il y a des coûts réels et quantifiables associés aux différents types de risques.

Les risques SI ne sont pas limités au périmètre interne de l'entreprise. Avec la complexité et l'ouverture croissante des systèmes d'information, une défaillance d'un partenaire peut avoir des répercussions importantes au sein du SI de l'entreprise et ses dirigeants peuvent être pénalement responsables des défaillances de la sécurité de leur SI. De même, le SI n'est pas limité au système informatique : l'information se présente sous des formes très variées en termes de stockage, de représentation et de transmission et le risque de perte d'informations sensibles (accentué par l'utilisation de mobile, portable, clé USB, web access,...) peut créer des pertes importantes de revenus.

La sécurité a une dimension humaine majeure : contrairement aux idées reçues, les attaques internes à l'entreprise ont le plus d'impact. La sécurité de l'information est donc une préoccupation collective qui doit être supportée par le management.

Les défaillances ne pouvant pas être évitées à 100 % à un coût raisonnable, la couverture des risques doit être planifiée en conséquence. La stratégie de gestion des risques du SI doit être alignée avec la gestion des risques globaux, et conforme au seuil de tolérance accepté par l'entreprise.

## >> Système de Gestion de la Sécurité de l'Information (SGSI) : les bénéfices attendus

Le principe de l'approche holistique est que le tout n'est pas égal à la somme de ses parties, mais relève d'une édification, organisation, intelligence dépassant toujours la somme des parties qui le composent. La gestion des risques du système d'information répond à ce principe. C'est bien par une gestion cohérente et transverse de l'ensemble des activités de l'entreprise, la motivation et la coordination de tous, que le risque global est le plus efficacement limité. Le risque du système d'information doit être intégré dans cette démarche.

(1) Approche globale.

La sécurité de l'information peut donc se définir comme un dispositif global de gestion des risques garantissant un niveau approprié de protection et assurant la disponibilité, l'intégrité, la confidentialité et la traçabilité de cet actif. Elle couvre un vaste domaine englobant la sécurité des systèmes d'information et des réseaux, la certification des échanges, la gestion des accès et des habilitations, la gouvernance, la protection vis-à-vis de l'intelligence économique, la classification des données, la gestion des actifs informationnels, la continuité de l'activité, la formation et la sensibilisation des acteurs.

La technologie ne peut résoudre seule tous les problèmes de sécurité. La solution repose sur une approche complémentaire aussi bien technique qu'organisationnelle. La gestion des risques apporte une justification rationnelle aux choix stratégiques. La convergence entre les méthodologies traditionnelles de gestion des risques et la gestion des risques du système d'information augmente en raison du gain financier potentiel. Ce dernier peut être réalisé par une meilleure priorisation des efforts de remédiation et pour les bénéfices inhérents, à une prise de décision fondée sur une bonne connaissance des risques. De plus, une gestion des risques appropriée, s'appuyant sur une norme reconnue, augmente le facteur de confiance des clients vis-à-vis de l'entreprise.

Les éditeurs ont compris l'intérêt d'une démarche globale et leurs nouveaux outils de « Governance, Risk, Compliance » (GRC) offrent une solution pour accompagner les entreprises. Cependant, ces outils ne peuvent être efficaces que si la politique risque est clairement établie, bien conçue, contrôlée et constamment améliorée. Le SGSI permet alors d'apporter des résultats concrets, durables, mesurables et proportionnés aux risques.

## >> Les bonnes pratiques : démarche, cadres et référentiels

La mise en œuvre d'une politique de gestion des risques du système d'information nécessite l'adhésion de la direction de l'entreprise. Elle s'inscrit dans une démarche itérative d'amélioration continue et peut s'appuyer sur des référentiels de bonnes pratiques reconnus (Norme ISO 2700X<sup>(2)</sup>, Méthodologies EBIOS<sup>(3)</sup>, MEHARI<sup>(4)</sup>, COBIT<sup>(5)</sup>,...).

Le modèle de SGSI proposé par la norme ISO 27001 est fondé sur une approche de gestion des risques définissant un ensemble de mesures de sécurité. Il permet d'assurer qu'une organisation de la sécurité de l'information est en place et s'inscrit dans un processus d'amélioration continue. Pour cela, la norme reprend le cycle « Plan Do Check Act »<sup>(6)</sup> de Deming, instancié à la sécurité des SI.

Aucune organisation ne peut maintenir son activité en éliminant tous les risques. A contrario, la prise de risques est créatrice de valeur si sa gestion est optimisée et permet son identification et sa quantification. L'entreprise peut ainsi définir en toute connaissance de cause de nouvelles opportunités et proposer de nouveaux produits avec des risques maîtrisés, une tarification optimale et donc un meilleur positionnement sur le marché. Il ne s'agit pas d'empêcher mais plutôt de faciliter la prise de risque dans une optique d'arbitrage risque/performance.

Du point de vue de l'entreprise, une gestion optimale des risques permet de contribuer :

- > D'une part, à la diminution de la volatilité des résultats grâce à la fixation de normes conduisant à une meilleure appréciation de toutes les dimensions des risques pris,
- > D'autre part, à une optimisation des fonds propres alloués à ses différentes activités.

Pour cela, il faut pouvoir évaluer et approcher le risque de manière cohérente dans toute l'organisation. Il est donc important de gérer les risques du système d'information à un niveau global en respectant les règles de gestion de l'entreprise. En adoptant cette vision globale, l'entreprise peut tirer parti de sa diversité et ainsi prendre plus de risques dans certaines activités à forte rentabilité.

La mise en œuvre d'un SGSI permet d'adopter cette vision holistique et de diffuser la culture risque à tous les niveaux de l'organisation. L'investissement initial de déploiement est vite compensé par l'optimisation induite de l'activité •

focus

### L'ANALYSE DES RISQUES EN SIX ÉTAPES PRINCIPALES

#### 1 Gouvernance en amont

Définit le cadre, les objectifs, le périmètre et valide les métriques de risque en accord avec la politique globale de l'entreprise. Cette étape a pour objectif d'établir les fondations d'une politique de gestion des risques commune, de définir un plan de communication et de mettre en œuvre un pilotage par les risques.

#### 2 Analyse des enjeux métiers

Permet de classer les ressources des processus clés de l'entreprise. Elle pourra être centrée sur les actifs critiques. Cette étape nécessite la participation des métiers (management opérationnel) et s'appuie sur une cartographie des quatre couches du système d'information : métier, fonctionnelle, applicative et technique.

#### 3 Diagnostic des vulnérabilités

Permet d'identifier la possibilité de concrétisation des menaces (potentialité et impact), de les quantifier et de distinguer les risques acceptables et inacceptables. Cette étape repose sur une analyse des processus transverses et nécessite la participation des directions centrales (DSI, DRH, Direction Juridique, Services Généraux,...).

#### 4 Traitement des risques

Les risques sont réduits, transférés, évités ou acceptés en fonction de critères préalablement définis.

#### 5 Planification, pilotage et mise en œuvre de processus de contrôles appropriés

Mesure l'efficacité du SGSI.

#### 6 Amélioration

Il est important de reconsidérer régulièrement le contexte de l'organisation, de remettre en cause la politique et les objectifs stratégiques et de réviser l'analyse des risques. Une nouvelle itération des différentes étapes précédentes permettra d'affiner le modèle de gestion des risques.

(2) Norme ISO 2700x : famille de normes pour la gouvernance sécurité - (3) EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité - (4) MEHARI : Méthode Harmonisée d'Analyse de Risques - (5) COBIT : Control Objectives for Information and Technology ou Démarche de pilotage des risques informatiques - (6) Méthode « Plan Do Check Act » (PDCA) est une méthode de gestion de la qualité.