ORGANISATION

Le positionnement du RSSI en question

Marie-Agnès Nicolet

Associée, directrice générale
Audisoft Consultants

La fonction de RSSI, définie par le Livre Blanc de 1996 sur la sécurité des systèmes d'information de la Commission bancaire, a été mise en place dans la plupart des établissements. Mais son positionnement n'est pas toujours clair dans les organisations bancaires.

À qui rattacher le RSSI ? Parmi les multiples impacts des dernières évolutions du CRBF 97-02, en mars 2005 (applicables au 1er janvier 2006), la place du responsable de la sécurité des systèmes d'information, ou RSSI, dans les dispositifs de contrôle interne constitue l'une des problématiques significatives posées aux organisations bancaires. Cette fonction, définie il y a une dizaine d'années par le Livre Blanc sur la sécurité des systèmes, a été mise en place dans la plupart des établissements bancaires, mais à des niveaux très différents de l'organisation.

JUGE ET PARTIE

Il n'est pas rare que cette fonction de pilotage de la sécurité des systèmes dépende encore du directeur des systèmes d'information (DSI). Même si certains établissements considèrent que ce rattachement – à la fois proche des opérationnels de la DSI et, en même temps, séparé d'eux – est une bonne solution, il rend son positionnement délicat en cas de dysfonctionnement grave en matière de sécurité nécessitant une alerte au plus haut niveau de l'organisation. Le directeur des systèmes d'information pourrait, en effet, être juge et partie et le RSSI manquer d'indépendance. Il est donc pertinent de séparer cette fonction de celle des DSI. Cette recommandation est souvent reprise par le régulateur, suite à des contrôles sur place.

Certains établissements ayant fait ce choix de séparation, la place du RSSI dans l'organisation n'est pour autant pas si simple à trouver. Avant la modification du CRBF 97-02, certains établissements avaient pu rattacher cette fonction à l'audit interne, l'une des facettes de cette fonction consistant à évaluer régulièrement le niveau de sécurité atteint, suivre la mise en place des plans d'action décidés par le comité sécurité ainsi que, le cas échéant, faire diligenter des audits spécifiques, comme un audit d'intrusion du réseau, par exemple. Mais, depuis la séparation des fonctions de contrôle permanent et périodique accompagnant la création de la fonction conformité, le positionnement du RSSI nécessite d'être repensé. Fait-il partie du contrôle permanent ou est-il une filière opérationnelle de pilotage de la sécurité ? C'est la question que se posent certains établissements.

Cette fonction à multiples facettes (*encadrés 1 et 2*), qui propose ou édicte des normes de sécurité, pilote les actions de sécurité, anime un comité présidé par un membre de la direction générale, joue un rôle d'alerte en cas de dysfonctionnement, évalue régulièrement et contrôle la sécurité des systèmes d'information, revêt bien ces deux aspects de pilo-

1. REPÈRES

RSSI et conformité

■ Les départements des banques en charge des systèmes d'information (comme d'ailleurs les structures spécialisées mises en place dans les groupes mutualistes) pour la mise en œuvre de nouveaux applicatifs, le choix d'outils externes ou le pilotage de projets d'implémentation de systèmes se posent à dessein la question de l'application des dispositifs visant à assurer la conformité. Or, pour ces structures, les principaux enjeux de conformité résident notamment dans l'application de l'article 14 du CRBF 97-02, des principes du Livre Blanc sur la sécurité des systèmes, ainsi que de la bonne application des lois CNIL, et des durées légales d'archivage des documents. Le rôle du RSSI dans la conformité des établissements bancaires, notamment sur ces points précis, est donc majeur. Le RSSI sera ainsi l'un des rouages permettant d'assurer la conformité des établissements.

2. REPÈRES

RSSI, nouveaux produits et contrôle des prestataires essentiels

■ Pour les établissements ayant donné une acception large à la notion de "nouveaux produits" en intégrant notamment dans cette notion les modifications significatives de processus ou d'organisation, il apparaît essentiel que le RSSI donne son avis avant toute nouvelle mise en place d'applicatif ou s'assure que les normes de sécurité à intégrer lors du choix de tout nouvel outil, sont respectées. Par ailleurs, il sera également impliqué dans la transposition des normes de sécurité définies pour la banque en obligations pour les prestataires essentiels définis à l'article 4 r du CRBF 97-02. Le RSSI devrait avoir un rôle à jouer dans la définition des indicateurs à suivre et dans l'analyse des reportings envoyés par le prestataire sur la sécurité.
Il serait également envisageable que, le cas échéant, le RSSI fasse diligenter un audit sécurité chez le prestataire, et à tout le moins, ait un entretien périodique avec le responsable sécurité de l'entreprise prestataire.

tage et de contrôle permanent qui ne sont pas antinomiques. D'autres filières de contrôle permanent, en effet, peuvent être amenées à proposer des normes tout en mettant en place des plans de contrôle. C'est le cas des autres filières de risques qui font partie intégrante du contrôle permanent.

RSSI, RISQUES OPÉRATIONNELS ET CONTINUITÉ D'ACTIVITÉ

Certains établissements ont récemment souhaité intégrer dans une même direction à la fois les risques opérationnels, le RSSI et le responsable du pilotage des plans de continuité d'activité.
Cette organisation apparaît tout à fait pertinente, dans le sens où l'évaluation des risques opérationnels ne peut réellement se faire sans la contribution active du RSSI pour l'évaluation de la sécurité des systèmes qui sera un des éléments à intégrer dans la cartographie des risques. Les risques liés aux pertes de confidentialité d'information, à la disponibilité du système d'information, à une piste d'audit déficiente, ou à la non-fiabilité et non-intégrité des données doivent être, en effet, analysés dans un premier temps par les métiers eux-mêmes, qui analyseront les impacts sur leurs processus. En revanche, lorsqu'il s'agira de définir des plans d'action pour couvrir les risques potentiels les plus importants, il sera nécessaire d'interroger le RSSI. Il pourra d'ailleurs utilement compléter ses propres plans d'action de sécurité, en les priorisant en fonction des impacts sur les métiers.
Par ailleurs, pour évaluer l'impact des risques liés aux scénarios majeurs de type catastrophe (destruction d'immeuble, incendie, attaque terroriste, crue de la Seine, indisponibilité sur plusieurs jours des réseaux téléphoniques, virus informatique de grande ampleur ou panne EDF de grande échelle), l'évaluation des dispositifs de continuité en place et le résultat des tests est un élément majeur de l'évaluation du risque.

3. DÉFINITION

Le risque maximal tolérable

■ Celui-ci a été défini dans le Livre Blanc de 1996 sur la sécurité des systèmes d'information de la Commission bancaire.
Il est la valeur limite, en millions de francs, imposée par la direction générale, de la part des fonds propres nets désirés et de celle de la capacité bénéficiaire prévisionnelle nette de l'année que la banque "accepte" de perdre (part des bénéfices pouvant absorber un sinistre), plus, éventuellement le montant des garanties accordées par les assurances en cas de sinistres informatiques.

« La séparation du RSSI et des directions informatiques n'implique pas forcément que ces dernières se dessaisissent des aspects opérationnels de la sécurité. »

VERS UNE ORGANISATION CIBLE

La séparation du RSSI et des directions informatiques n'implique pas forcément que ces dernières se dessaisissent des aspects opérationnels de la sécurité, comme le suivi quotidien des tentatives d'intrusion ou des habilitations informatiques, et la mise en œuvre des actions décidées par le comité sécurité.
À terme, on pourrait imaginer la coexistence d'un ROSSI (responsable opérationnel de la sécurité des systèmes d'informations) rattaché à la DSI, et interlocuteur privilégié du RCSSI (responsable du contrôle de la sécurité des systèmes d'informations), quant à lui, rattaché au contrôle permanent de second niveau. Le RCSSI serait ainsi en charge des actions normatives et de pilotage, du *reporting* à la direction générale, de l'animation du comité sécurité, ainsi que de l'évaluation régulière de la sécurité et de ce fameux "risque maximal tolérable" (*encadré 3*) dont le concept a émergé il y a déjà plus de 10 ans. ■