LA FONCTION RSSI
Dix ans après sa création

Jacques Sarrasin

Animateur du groupe de travail "le RSSI, dans les faits, dix ans après le Livre Blanc"
Forum des Compétences
RSSI
LCL

Où en est la fonction de responsable de la sécurité du système d'information (RSSI) dix ans après sa naissance ? Les conclusions du Forum des Compétences sur ce point permettent de dégager les missions que la majorité des RSSI assument, celles qui sont déclarées hors-champ et celles qui font encore débat.

Où en est la fonction de responsable de la sécurité du système d'information (RSSI) dix ans après sa naissance ? À partir de nos expériences diverses et du recul acquis, un groupe de travail ("Le RSSI dans les faits, 10 ans après le Livre Blanc") a été créé pour faire le point sur ce sujet au sein du Forum des Compétences*.

Depuis dix ans, l'environnement du RSSI s'est complexifié. Sous l'autorité de la direction générale, en appui du contrôle permanent, sa mission l'a conduit à travailler avec les directions métiers de la banque ainsi qu'avec la direction informatique, en bénéficiant du support des directions de la communication, des ressources humaines et de la direction juridique, en collaborant avec les risques opérationnels, les assureurs et la conformité, en dialoguant avec le contrôle périodique. Tout en respectant les directives de la Commission bancaire, en s'appuyant sur le Livre Blanc, Bâle II, le CRBF 97-02, les normes, sans oublier la CNIL, l'AMF, le CFONB, la BRI... et le tableau est loin d'être complet.

Le RSSI assume une fonction transversale par excellence. Son environnement est marqué par une accélération des changements : les systèmes d'information sont, notamment, de plus en plus ouverts sur l'extérieur.

COMMENT AVONS-NOUS PROCÉDÉ ?

Pour réaliser cette étude, le Forum a recensé auprès de ses membres, les différentes missions unitaires assurées par les uns et les autres ; celles-ci ont été classées par thèmes. Puis un questionnaire a été réalisé et il a été demandé à chaque RSSI de se positionner par rapport à ces missions. Les résultats ont été dépouillés et trois catégories ont émergé : les missions que la majorité des RSSI déclare assurer, celles qui sont hors-champs et celles qui font l'objet de débats au sein du groupe de travail.

QU'EN EST-IL AUJOURD'HUI ?

Il apparaît que les RSSI sont les rédacteurs de la politique de sécurité du système d'information et des chartes relatives à la sécurité du système d'information.

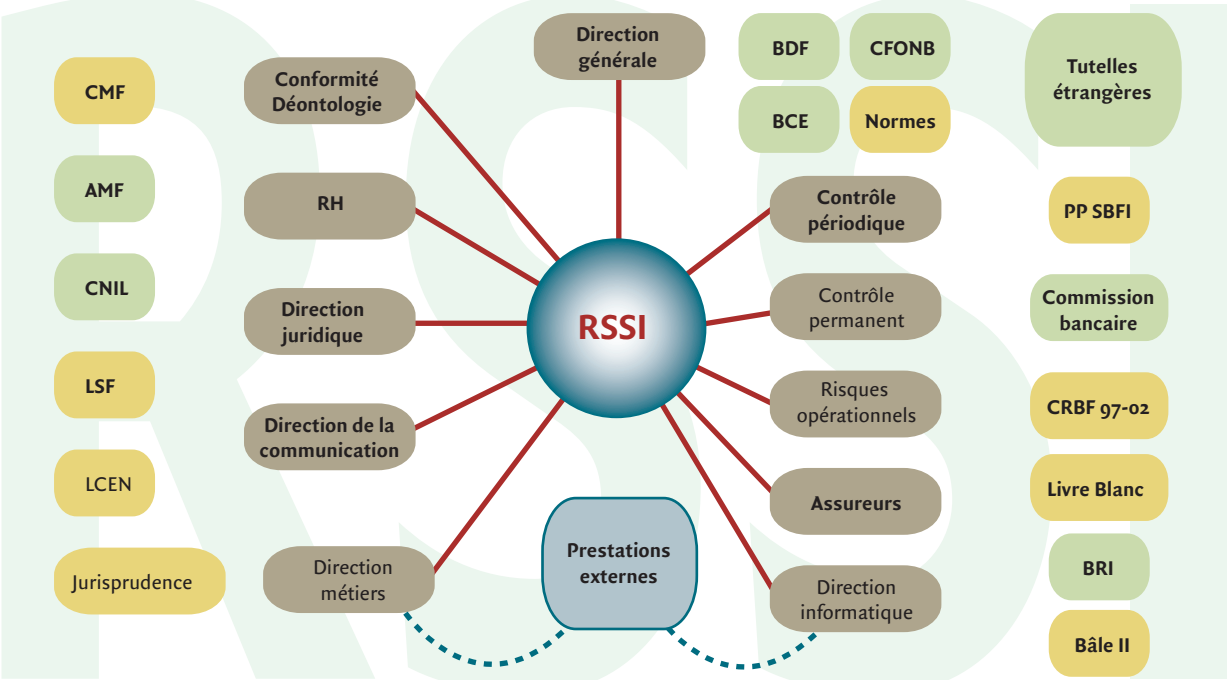
Ils participent à des comités de sécurité de haut niveau présidés par la direction générale ou un membre du comité de direction générale. C'est ici qu'ils exercent une part significative de leur devoir d'influence. Ils assistent également au comité de pilotage des grands projets informatiques ; ils contribuent à l'élaboration des plans de continuité d'activité (PCA) et sont membres de cellules de crise décisionnelles.

En aval de ces instances décisionnelles, ils animent dans les métiers bancaires, des réseaux de correspondants sécurité du système d'information et jouent auprès de ces derniers, un rôle de conseiller. Ils ont une fonction de sensibilisation et de conception des formations SSI. L'idéal serait que la SSI fasse systématiquement partie du contenu des formations normales pour un poste. Les RSSI participent aux formations, en tant qu'animateurs ou coanimateurs. En matière de contrôle, les RSSI sont promoteurs et acteurs du contrôle permanent. Ils animent, par exemple, une auto-évaluation de la sécurité du

> *« L'idéal serait que la SSI fasse systématiquement partie du contenu des formations normales pour un poste. »*

* Le Forum des Compétences a prévu une rencontre événementielle où il communiquera sur les fiches issues des travaux du groupe.

LA SPHÈRE D'INTERVENTION DU RSSI AUJOURD'HUI



Source : Forum des Compétences.

Légende :

AMF : Autorité des marchés financiers

BRI : Banque des règlements internationaux

CNIL : Commission nationale de l'informatique et des libertés

BCE : Banque centrale européenne

LCEN : Loi pour la confiance dans l'économie numérique

CMF : Code monétaire et financier

PP SBFI : Profil de protection pour services bancaires et/ou financiers sur Internet

CFONB : Centre français d'organisation et de normalisation bancaires

LSF : Loi sur la sécurité financière

RH : Ressources humaines

BDF : Banque de France

système d'information. Ils contribuent au rapport de contrôle interne réglementaire pour son volet "système d'information" et peuvent être amenés à le présenter au comité d'audit, dont ils ne sont cependant pas membres.

En revanche, le RSSI n'est pas prescripteur, ni acheteur d'une solution technique qui doit se conformer à ce qui est défini dans la politique SSI. Il n'est pas pas non plus le gestionnaire de composants techniques. Enfin, il ne fait pas partie de l'organe du contrôle périodique : sa mission peut naturellement être auditée et inspectée.

Entrer ces deux bornes, se décline un certain nombre de missions qui font l'objet de débats sur le fait de savoir si elles relèvent ou non du poste du RSSI. Les situations varient en fonction de chaque établissement, mais visent en général à établir un équilibre harmonieux entre les prérogatives du RSSI, du responsable des PCA et de celui des risques opérationnels dont la fonction a été créée le plus souvent bien après le Livre Blanc.

LE PORTRAIT-ROBOT DU RSSI

Le RSSI est un homme ou une femme d'expérience qui assure une fonction transversale. Il ou elle doit avoir des qualités de communiquant et se poser comme un facilitateur. Sa fonction s'exerce pour prévenir un danger. Son efficacité se mesure au travers de la maîtrise des risques SI par l'entreprise. Son action et celle de ses correspondants au sein de l'entreprise doivent permettre aux différents acteurs de connaître les risques encourus, de les réduire et d'assumer les risques résiduels.

Sa position au sein de la société dépend de l'histoire, de la culture de l'entreprise, mais aussi de sa taille. Il ne peut être réellement efficace pour l'entreprise que s'il est proche de la direction générale. Le RSSI aura réussi sa mission si la maîtrise des risques SI est tellement intégrée à la vie de l'entreprise qu'il n'y a plus nécessité absolue d'une animation spécifique. Il y a dix ans nous pensions pouvoir le faire en quatre ans. C'est encore le cas aujourd'hui ! Excès d'optimisme ? ■