

Le rôle du RSSI (Responsable de la Sécurité des Systèmes d'Information)

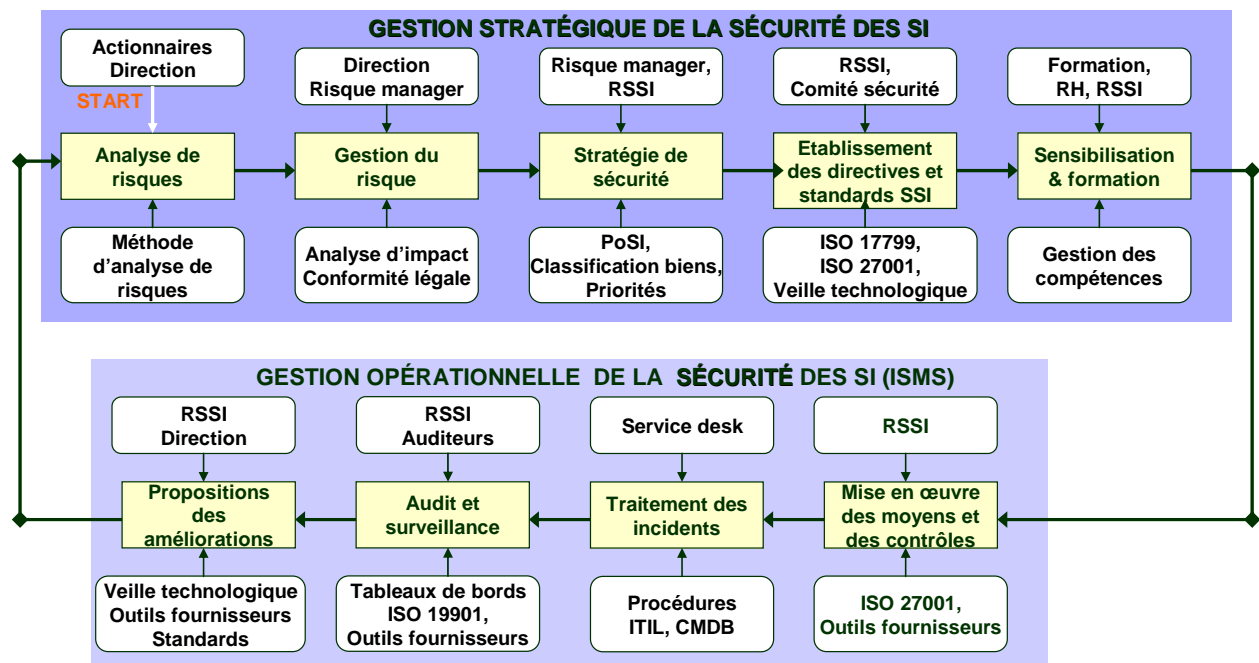
Claude Maury

Président CLUSIS

Association suisse de la sécurité des Systèmes d'Information (SI)

Pour beaucoup de directions d'entreprises, le rôle du RSSI est d'être le garant de la politique de sécurité des systèmes d'information (SSI). Ce dernier est confiné dans la gestion technologique et administrative des mesures de sécurité mises en œuvre ou à mettre en œuvre.

En réalité, comme pour la gestion de la qualité selon ISO 9000, la sécurité des systèmes d'information est un processus business qui commence bien en amont de la simple gestion de la technologie informatique utilisée pour protéger l'information de l'organisation.



Processus de la sécurité des systèmes d'information

Le rôle du RSSI est de définir, mettre en œuvre et contrôler le processus de sécurité des systèmes d'information basé sur une architecture de sécurité et une politique de sécurité des SI.

Le RSSI participe directement avec le Risk Manager à la définition de la stratégie de sécurité nécessaire pour couvrir les risques et les impacts sur les biens informationnels de l'organisation. Cette stratégie se traduit par la définition d'une architecture de sécurité des SI.

Une architecture de sécurité est un plan et un ensemble de principes, de directives, de procédures et de standards qui décrivent :

- Les services de sécurité nécessaires à un système lui permettant de satisfaire les besoins de ses utilisateurs
- Les éléments du système nécessaires à la mise en œuvre des services de sécurité
- Les niveaux de performance exigés pour répondre aux menaces

Une architecture complète de sécurité de l'information inclut la sécurité administrative, la sécurité des informations, la sécurité des matériels et logiciels, la sécurité du personnel et la sécurité physique de l'environnement.

Une architecture complète de sécurité doit traiter les genres de menaces intentionnelles, intelligentes et accidentelles.

Une campagne de sensibilisation à la SSI pour tout le personnel de l'organisation, quel que soit son niveau professionnel, doit supporter ce processus de SSI afin que chacun en comprenne l'importance et les enjeux.

Le processus de gestion opérationnel de la SSI ne peut être mis en œuvre efficacement que lorsque tout le processus stratégique de la SSI est entièrement supporté par la direction de l'organisation. La norme ISO 27001 décrit très bien ce processus opérationnel selon le principe de la roue de Deming. Dans ce cas, une synergie de compétences et de ressources est possible avec l'équipe qualité ISO 9000 de l'organisation.

Le RSSI doit aussi pouvoir s'appuyer sur des compétences techniques et théoriques, un audit interne ou externe et un comité SSI représenté par des responsables des secteurs business. Il doit aussi être partie prenante du « Change Advisory Board », lorsque l'organisation est engagée dans un processus ITIL.