Auteur : Lionel GUILLET
Expert en Management de la Sécurité de l'Information

Sécurité de l'information :
DEFINIR ET ORGANISER LES ROLES ET LES RESPONSABILITES

Qui fait quoi en matière de Sécurité de l'Information ?

Tout commence par une bonne organisation, une organisation qui ne s'accommode pas des confusions et des ambiguïtés de responsabilités et du pilotage à vue.

Cette "vérité" générale s'applique selon des modalités particulières à la gestion de la Sécurité de l'Information, avec l'approche spécifique que celle-ci exige.

Et le présent article n'a pas d'autre ambition que de vous proposer quelques éléments, à partir d'une analyse et d'un retour d'expérience personnels, et de susciter vos réactions et vos commentaires sur le sujet.

En effet, une dissertation sur l'organisation et le management de la Sécurité de l'Information mérite d'être complétée, ou plutôt d'être enrichie, de l'apport de connaissances et d'analyses tierces.

La définition et l'organisation des responsabilités en matière de Sécurité de l'Information constituent le socle indispensable d'une gestion efficiente et pérenne

C'est une des actions fondatrices du Système de Management de la Sécurité de l'Information (S.M.S.I.) à mettre en place pour garantir le pilotage et le management de la démarche comme nous l'évoquons dans l'article consacré au sujet. (Pour inscrire le PCA dans la durée - Piloter la sécurité de l'information de l'entreprise)

IL S'AGIT, EN EFFET, DE DEFINIR L'ORGANISATION QUI DOIT PERMETTRE L'APPROCHE GLOBALE STRUCTUREE DE L'ENSEMBLE DES GESTIONS INDISPENSABLES A L'EVALUATION ET A LA PROGRESSION CONTINUE DE LA SECURITE DE L'INFORMATION DANS TOUTES LES ACTIVITES DE L'ENTREPRISE.

CETTE ACTION EST STRATEGIQUE. ELLE APPARTIENT AUX STRUCTURES D'ADMINISTRATION ET DE DIRECTION DE L'ENTREPRISE QUI DISPOSENT POUR CELA D'UN CADRE NORMATIF A ADAPTER A LEUR CONTEXTE.

En effet, engagement au plus haut niveau, attribution des responsabilités, coordination et évaluation des actions … les normes Iso 27001 et 27002 font valoir les objectifs et les mesures à retenir pour définir un modèle de gouvernance de la sécurité, mais, sans en préconiser un particulièrement.

C'est logique, **IL S'AGIT, NON DE REMETTRE EN CAUSE L'ORGANISATION EXISTANTE, MAIS, DE S'APPUYER SUR ELLE POUR REPONDRE AUX EXIGENCES PARTICULIERES DE LA DEMARCHE, A SA TRANSVERSALITE MULTIDISCIPLINAIRE**.

La Sécurité de l'Information, ce n'est pas l'affaire d'un homme seul

C'est **L'ERREUR** à éviter, confier la responsabilité de "faire de la sécurité" à une seule personne.

Au plan stratégique et décisionnel comme au niveau fonctionnel et opérationnel, la Sécurité de l'Information doit fédérer toutes les responsabilités, toutes les compétences de l'entreprise en devoir d'en connaître par référence à la législation et à son champ d'application.

Et c'est là qu'il est impératif d'ordonner cette pluralité des intervenants sous peine de voir la démarche se perdre dans les sables.

Pour cela ? Rien d'original. Instances de contrôle et de décision, maîtrise d'ouvrage et maîtrise d'œuvre font parfaitement l'affaire. Et c'est l'organisation existante qui sert à la désignation des acteurs dans le respect de leurs responsabilités respectives.

Une instance de décision dirigeante

Le pilotage doit être assuré par la direction de l'entreprise compte tenu des enjeux et du champ couvert par la démarche. Ainsi, un comité composé de l'ensemble des directeurs est naturellement instance d'arbitrage et de décision **POUR** :

- Intégrer les problématiques de sécurité dans la gouvernance générale de l'entreprise
- Déterminer la stratégie de l'Entreprise en matière de Sécurité de l'Information
- Décider des plans d'actions à entreprendre sur proposition de la maîtrise d'ouvrage déléguée
- Evaluer les résultats des plans d'action mis en œuvre et le niveau de sécurité de l'entreprise par le biais d'indicateurs spécifiques
- Rendre compte aux administrateurs de la gestion des risques, le cas échéant

Une collaboration étroitement complémentaire entre une Maîtrise d'ouvrage et une Maîtrise d'œuvre

Sur le plan fonctionnel et opérationnel, les gestions reposent sur le travail en parfaite collaboration d'une maîtrise d'ouvrage et d'une maîtrise d'œuvre plurielle.

Sur délégation, formelle et publiée, du directeur général, la (les) personne(s) désignée(s) à **LA MAITRISE D'OUVRAGE** Sécurité de l'Information **A** (ont) toute **LEGITIMITE POUR** :

- Garantir le respect des objectifs de sécurité de l'entreprise
- Assurer l'information et la sensibilisation des partenaires et des utilisateurs de son système d'information
- Identifier les risques et les vulnérabilités du système d'information
- Coordonner et évaluer la mise en œuvre des mesures et des actions de sécurité
- Accompagner les maîtrises d'œuvre dans la prise en compte des référentiels de Sécurité
- Conseiller et alerter la direction de l'entreprise
- Procéder à une veille informationnelle spécifique

Quant à **LA MAITRISE D'ŒUVRE**, elle **A POUR ROLE DE** :

- Définir, formaliser, mettre en œuvre et maintenir les dispositions et solutions de sécurité de l'information
- Participer à la maîtrise des risques opérationnels des activités placées sous sa responsabilité
- Assister la maîtrise d'ouvrage dans l'expression des besoins de sécurité.

Mais, la maîtrise d'œuvre n'est pas une, elle est multiple, nous l'avons déjà souligné plus haut.

Elle est composée de l'ensemble des Directions et des Services de l'entreprise acteurs à la Sécurité de l'Information, dans les 11 domaines limitativement énumérés à la norme Iso 27001, depuis la sécurité des ressources humaines jusqu'aux sécurités juridiques, en passant par les sécurités physiques, la continuité de service, les sécurités informatiques et autres … (voir l'annexe à l'article "Piloter et manager la Sécurité de l'Information).

Une Instance de contrôle

Périodiquement, au moins une fois par an, il convient de procéder à l'évaluation du niveau de sécurité de l'entreprise et de l'efficacité des mesures et des actions mises en œuvre pour la maintenir et l'améliorer.

Solution interne ou externe, mais, il faut donc identifier également, dans l'organisation, la structure, la (les) personne(s) habilitée(s) à exercer cette évaluation.

S'il existe un contrôle interne dans l'entreprise, comme la législation le prévoit pour certaines au nom de la sécurité financière et de la certification des comptes, celui-ci, chargé de gérer la prévention des risques, peut intégrer le suivi des risques attachés à la Sécurité de l'Information dans sa mission originelle.

Une identification clairement établie des responsabilités pour éviter les conflits d'intérêts et la confusion des interventions

Donc, la maîtrise d'ouvrage exprime les besoins de sécurité et les maîtrises d'œuvre conçoivent et réalisent les actions.

Cette distinction doit être clairement établie, non pas pour séparer, mais pour éviter les confusions de responsabilités et les conflits d'intérêts et afin de garantir la complémentarité des interventions, une complémentarité indispensable dans cette démarche parfaitement transversale et multidisciplinaire.

Aussi, est-il souhaitable que la maîtrise d'ouvrage et tous les partenaires à la maîtrise d'œuvre Sécurité de l'Information se retrouvent régulièrement pour favoriser leurs échanges et la bonne coordination des interventions.

Une organisation qui peut associer qualité & sécurité avec profit

L'organisation mise en place doit répondre, il faut le souligner, aux besoins d'une démarche dynamique d'amélioration continue dont l'objectif est d'atteindre un système conforme à des objectifs de sécurité préalablement définis.

C'EST UN PROCESSUS QUI PEUT PARFAITEMENT S'ASSOCIER A UNE APPROCHE QUALITE, CAR ETROITEMENT COMPLEMENTAIRE DE CELLE-CI SANS POUVOIR ETRE CONFONDU AVEC ELLE, CAR BASE SUR UN REFERENTIEL DISTINCT.

Il n'en demeure pas moins que, dans l'hypothèse où l'entreprise s'engage, ou est déjà engagée, dans une approche qualité, les responsables d'activités, désignés à ce titre, peuvent être également maîtrise d'œuvre à la Sécurité de l'Information dans leur domaine de compétences.

Cette option a pour mérite de proposer une cohérence d'ensemble favorable à la maîtrise des risques opérationnels dans les activités.

Un réseau de correspondants locaux pour garantir l'unité de gestion de la Sécurité de l'Information

Dans les entreprises décentralisées, la mise en place d'un réseau de correspondants locaux à la Sécurité de l'Information ne peut que faciliter l'homogénéisation des pratiques et des contextes et la bonne circulation de l'information, notamment lors de la gestion d'incidents de sécurité.

Une approche R.A.C.I pour faciliter l'identification des intervenants

Organiser le management de la Sécurité de l'Information, plus facile à dire qu'à faire feront observer fort justement certains à la lecture de cet article.

C'est vrai. Aussi pour aider à la définition des rôles, il est possible d'utiliser une approche basée sur une matrice de responsabilités, dite matrice R.A.C.I., à partir des initiales des mots qui lui donne son sens :

R C'est le Responsable, nominativement identifié, de la mise en œuvre d'une action, d'une solution, d'une mesure, d'une procédure …. Plusieurs "R" sont possibles, mais, dans ce cas, il faut désigner le "R" qui conduit l'opération

A c'est l'Autorité approbatrice, en général le Directeur, celui qui sera responsable en cas de carence.

C désigne les partenaires consultés dans leur domaine d'expertise

I identifie les personnels informés parce qu'impactés par l'action

Ainsi, cette matrice, appliquée à votre organisation, doit vous permettre d'identifier les partenaires à une intervention

Un exemple –
Le Directeur, **A**utorité responsable, décide de la sécurisation des accès à des locaux sensibles.
Cette action est **R**éalisée par le Responsable du Service habilité à le faire.
Le Manager de la Sécurité de l'Information est **C**onsulté et associé à son suivi.
Les personnels et les visiteurs sont **I**nformés de cette disposition et de ces implications en termes opérationnels

La démarche s'applique à toutes les entreprises quelle que soit leur taille

Une gouvernance, des instances d'échanges, des rôles distincts … l'article pourrait laisser penser que l'organisation du management de la Sécurité de l'Information n'intéresse que les entreprises de grande dimension. Pas du tout.

La norme Iso 27001 le prévoit bien.

Sur une seule personne, sur plusieurs, sur un service, l'essentiel est que l'ensemble des activités structurantes , arbitrage et décision, management des risques, réalisation et mise en œuvre, évaluation et contrôle, soient garanties dans un cycle d'amélioration continue de la Sécurité de l'Information appréhendée dans son ensemble.

IL est vrai que ce n'est pas la taille de l'entreprise qui dicte les besoins de sécurité, ce sont les enjeux métiers, les obligations et les engagements de service, la sensibilité des actifs de l'entreprise, les contraintes juridiques …

Pas de confusion entre la Responsabilité des Sécurités informatiques et le management de la Sécurité de l'Information

Le débat est ouvert depuis longtemps. Il ne faut pas qu'il porte préjudice à la bonne conduite des gestions.

Pour éviter ce risque, il ne faut surtout pas oublier, que le management de la Sécurité de l'Information n'intéresse pas que les seules sécurités informatiques, mais que celles-ci occupent une place particulière dans le dispositif.

C'est ainsi qu'UN RESPONSABLE DE LA SECURITE DES SYSTEMES D'INFORMATION, UN R.S.S.I., selon l'appellation métier labellisée, EST UN EXPERT EN … SECURITES INFORMATIQUES et qu'IL NE DOIT PAS ETRE CONFONDU AVEC UN MANAGER DE LA SECURITE DE L'INFORMATION CHARGE D'UNE APPROCHE GLOBALE DES RISQUES, DE TOUS LES RISQUES, pas seulement des risques informatiques, et ceci, sous l'angle maîtrise d'ouvrage.

Or, pour le sujet qui nous intéresse, dans une répartition des rôles bien comprise, chaque métier gère ses risques, l'organisation doit être basée sur ce principe.

Par conséquent, le R.S.S.I. gère ceux de la Direction informatique sous l'autorité de son directeur.

Mais, dans un contexte où l'entreprise est étroitement dépendante du bon fonctionnement et de la performance de son système d'information informatique, le R.S.S.I., outre ses responsabilités fonctionnelles et

opérationnelles pourra être justement associé à la définition et la gestion générales des mesures et des actions de sécurité de l'information, pour apporter son expertise dans leur traitement et étudier leurs interactions avec son champ de responsabilité, afin que l'informatique soit en phase avec les objectifs de l'entreprise.

Ainsi, dans l'intérêt de l'entreprise, manager de la Sécurité de l'Information et responsable de la sécurité des systèmes d'information doivent travailler ensemble à la définition d'actions communes dans lesquelles l'Informatique est partie prenante.

Et dans une entreprise à effectif réduit alors, comment faire, puisque l'approche normative est valable pour toutes les organisations, les grandes et les moins grandes ?

Les fonctions de manager des risques informationnels et de responsable des sécurités informatiques peuvent être confiées à la même personne lorsque le contexte l'exige. Une condition cependant, il faut que l'intéressé, la direction, toute l'organisation, restent attentifs à maintenir dans les gestions la séparation des rôles.

Un Responsable de la fonction Plan de Continuité d'Activité

Dans le dispositif, il ne faut pas oublier la désignation d'un responsable de la fonction Plan de Continuité d'Activité dès que l'entreprise s'engage dans cette démarche, une désignation inscrite dans les conseils publiés par Robert BERGERON sur le sujet (10 conseils pour réussir son PCA), une désignation indispensable au maintien en conditions opérationnelles de la continuité de service de l'entreprise.

Bien sûr, ce responsable de processus travaillera également en étroite collaboration avec la Maîtrise d'Ouvrage à la Sécurité de l'Information. Rien ne s'oppose d'ailleurs à ce que ce soit la même personne, compte tenu de l'exigence de transversalité que sa fonction demande également. Rien ne s'y oppose, mais, rien ne le justifie non plus.

Définir, mais aussi publier l'organisation dédiée à la Sécurité de l'Information

La publication de l'organisation du pilotage et du management de la Sécurité de l'Information de l'entreprise participe à la construction, si essentielle, de la légitimité de la démarche auprès de l'ensemble des personnels.

Elle a pour avantage également de formaliser, à l'attention de tous les partenaires, les attributions de chacun et des organes de décision et de suivi de la Sécurité de l'Information.

Une conclusion qui n'en est pas une

L'intégration du pilotage et du management de la Sécurité de l'Information dans les objectifs de l'entreprise est un projet collectif et structurant qui s'adresse à toutes les Directions et tous les Services intéressés à sa mise en œuvre.

Mais, il est certain que, pour être pleinement efficace, cet engagement doit être partagé par tous.

Et c'est là que la communication, par l'information et la sensibilisation de tous les membres du personnel et de tous les utilisateurs du système d'information de l'entreprise se révèle également un volet essentiel de la démarche.

Mais, c'est un autre sujet … d'article.

Et vos observations et vos questions qui nous intéressent

Cet article doit susciter des observations et des questions à sa lecture.

Ne nous en privez pas, ne serait-ce que pour l'enrichir de vos commentaires et de vos expériences.

Pour cela, vous avez une adresse électronique à votre disposition guillet.lionel@gmail.com