

Quel avenir en 2010 pour le domaine de la Sécurité de l'Information au Luxembourg ?

(Document de Synthèse)

Résumé

Le présent document expose le résultat d'une réflexion structurée, menée par **des professionnels du domaine de la Sécurité de l'Information** qui se sont attachés à **analyser l'évolution spécifique de 4 métiers du domaine de la Sécurité de l'Information au Grand-Duché du Luxembourg d'ici 2010**. Cette réflexion s'inscrit pour rappel dans le cadre d'un projet européen interrégional, le Projet Abilitic¹. Les métiers étudiés sont les suivants :

- **Le métier d'Auditeur en Sécurité de l'Information**
- **Le métier de Consultant en Sécurité de l'Information**
- **Le métier d'Ingénieur – Chargé de monitoring des incidents IT**
- **Le métier de Juriste en Sécurité de l'Information**

En fonction de l'horizon ciblé, c'est-à-dire à horizon 3 – 5 ans, ces professionnels ont construit ensemble des hypothèses d'évolution pour le domaine de la Sécurité de l'Information. Ils ont ensuite mesuré l'impact de ces hypothèses sur les compétences existantes des métiers. **Une vingtaine de compétences a été identifiée comme clés** pour les trois à cinq ans à venir pour chacun des métiers. Les professionnels consultés ont complété leur réflexion par un travail de projection sur les éléments nouveaux (compétences, responsabilités, prérogatives) que la vision de chacun des métiers traités devra intégrer à moyen terme. A ce titre, **une dizaine de compétences nouvelles a été recensée pour chaque métier**.

Tout au long du processus du projet Abilitic, une démarche participative a été proposée aux experts du domaine de la Sécurité de l'Information. A ce titre, l'équipe du projet Abilitic tient à remercier l'ensemble des acteurs qui ont participé à cette réflexion.

Mots-clés : Compétences, Sécurité de l'Information, anticipation, prospective

CITI

Centre de Recherche Public Henri Tudor
29, Avenue John F. Kennedy
L-1855 Luxembourg - Kirchberg
Tél.: +352 42 59 91 - 333
Fax: +352 42 48 99

Rédigé par Bertrand Meunier¹, Duan Hua², Frédéric Girard³,

¹bertrand.meunier@tudor.lu - Chef de projet

²duan.hua@tudor.lu - Expert méthode

³frédéric.girard@tudor.lu - Reviewer

www.citi.tudor.lu

¹ Pour de plus amples renseignements, consultez le site www.abilitic.eu

Remerciements

L'équipe du projet Abilitic adresse ses remerciements à :

Monsieur **Yuri AUFFINGER**, Cabinet Reisch & Verlainé Avocat
Monsieur **Claude ARBOGOAST**, CEI
Monsieur **Philippe BACH**, Fortis Banque Luxembourg
Monsieur **Maurice BAUER**, CETREL
Monsieur **Roland BOMBARDELLA**, Haut Commissariat à la protection nationale
Monsieur **Malike BOUAOUD**, IT WORKS
Monsieur **Thorsten BRAUN**, Luxinnovation.lu
Monsieur **Philippe DANN**, UBIZEN
Madame **Muriel DEBIENNE**, ING
Monsieur **Charles DELBRASSINE**, IT WORKS
Monsieur **Benoît DELOBBE**, CETREL
Monsieur **Eric DUBOIS**, CRP Henri Tudor
Monsieur **Jean - Marie DEOM**, Banque du Luxembourg
Monsieur **Yves DE PRIL**, Conostix
Monsieur **Alexandre DULAUNOY**, SES ASTRA
Monsieur **Christophe FELTUS**, CRP Henri Tudor
Monsieur **Raymond FABER**, Ministère de l'Economie et du Commerce Extérieur
Madame **Sylviane FRANCAERT**, Fortis Banque Luxembourg
Monsieur **Frédéric GIRARD**, CRP Henri Tudor
Monsieur **David HAGEN**, CSSF
Monsieur **Emile HAZAN**, Avocat
Monsieur **Olivier HEMROULLE**, Ubizen
Monsieur **Romain HILBERT**, Dimension Data Luxembourg
Monsieur **Jean-Philippe HUMBERT**, OLAS
Monsieur **Jean-Yves KAYSER**, Chambre des Métiers
Monsieur **Belkacem KECHICHEB**, CRP Henri Tudor
Monsieur **Djamel KHADRAOUI**, CRP Henri Tudor
Monsieur **Michel LAURENT**, Electrolux Luxembourg
Monsieur **Cédric MAUNY**, TELINDUS
Monsieur **Koen MARIS**, Conostix
Monsieur **Laurent MELLINGER**, SECARON
Monsieur **René MOES**, Police Grand-Ducale du Luxembourg
Monsieur **Michel MOUREAU**, Econocom
Madame **Clara MULLER**, P&T
Madame **Sandrine MUNOZ**, BIL
Madame **Noëlle PELTIER**, CRP Henri Tudor
Monsieur **Cyril PIERRE-BEAUSSE**, Cabinet Allen & Overy Avocats
Monsieur **Sébastien POGGI**, CRP Henri Tudor
Monsieur **Alexandre ROSEVEGUE**, BNB Parisbas
Monsieur **Erwin SOTIRI**, Cabinet Legoueff Avocats
Monsieur **Pascal STEICHEN**, Ministère de l'Economie et du Commerce Extérieur
Monsieur **Thomas TAMISIER**, CRP Gabriel LIPPMANN
Madame **Florence THIEL**, Crédit agricole
Monsieur **François THILL**, Ministère de l'Economie et du Commerce Extérieur
Monsieur **Jean TRIMBOUR**, Luxinnovation.lu
Monsieur **Johan VAN DAMME**, Cours Européenne des Comptes
Monsieur **Jean Marie VERLAINE**, Cabinet Reisch & Verlainé Avocats
Monsieur **Stéphane WALRAVE**, Intrasoft International SA
Monsieur **Pierre WEIMERSKIRCH**, Commission Nationale pour la Protection des Données

Pour leur contribution, et leur participation active aux différents Groupes de Travail du projet Abilitic sur la sécurité de l'information au Grand-Duché du Luxembourg.

Table des matières

Introduction	4
Partie 1 : Méthodologie	5
Partie 2: Le profil d'évolution du domaine de la Sécurité de l'Information	6
1. Le Scénario d'évolution	6
2. Le plan d'action	7
Partie 3 : L'identification des compétences clés et nouvelles des métiers étudiés	12
1. Rappel :	12
A. La structure des profils professionnels.....	12
B. L'impact du scénario d'évolution sur le profil professionnel des métiers de la Sécurité de l'Information	12
C. L'identification des compétences clés et nouvelles des quatre métiers étudiés pour le domaine de la Sécurité de l'Information	12
2. Les résultats	13
A. Pour le métier d'Auditeur en Sécurité de l'Information	13
Les activités principales et tâches associées	13
Les compétences de l'Auditeur en Sécurité de l'Information	14
B. Pour le métier de Consultant en Sécurité de l'Information.....	16
Les activités principales et tâches associées	16
Les compétences du consultant en sécurité de l'information	17
C. Pour le métier d'Ingénieur - Chargé de monitoring des incidents IT.....	20
Les activités principales et tâches associées	20
Les compétences de l'ingénieur – chargé de monitoring des incidents IT	21
D. Pour le métier de Juriste en Sécurité de l'Information.....	24
Les activités principales et tâches associées	24
Les compétences du juriste en sécurité de l'information.....	25
Références	28

Introduction

A partir de 2003, le Centre de Recherche Public Henri TUDOR a souhaité développer une expertise en matière d'utilisation des outils qui sont ceux de la prospective (Godet, 2001) et de l'exploration des futurs longs. Le choix a été fait d'exploiter ces outils pour la conception et le développement de démarches d'anticipation des futurs « moyens » qui soient participatives et structurées. Participatives, car elles réunissent en présentiel une communauté d'experts ayant pour objectif d'exprimer, partager et évaluer leurs idées. Structurées, car elles mobilisent de manière amendée les outils traditionnels de la prospective pour l'évaluation et la sélection des idées.

C'est dans ce cadre que le Centre de Recherche Public Henri TUDOR a défini une démarche d'anticipation (Durand, 2004). Celle-ci a pour objectif d'identifier aujourd'hui les compétences dont des professionnels auront besoin demain, à moyen terme (3-5 ans). Le présent document a donc pour objectif de montrer qu'il est possible d'envisager le déploiement d'un tel exercice pour quatre métiers dans le domaine de la Sécurité de l'Information.

Les réflexions menées par les professionnels de la Sécurité de l'Information ont permis d'aboutir à l'identification des mutations que devrait connaître l'environnement du domaine étudié à horizon 2010. L'ensemble de ces mutations compose le scénario d'évolution. Les professionnels ont mesuré l'impact des changements du scénario d'évolution sur les compétences actuelles des quatre métiers sélectionnés :

- Le métier d'Auditeur en Sécurité de l'Information,
- Le métier de Consultant en Sécurité de l'Information,
- Le métier d'Ingénieur Chargé de monitoring des incidents IT,
- Le métier de Juriste en Sécurité de l'Information.

Ils ont abouti à l'identification des compétences clés que chacun des métiers devra être en mesure de maîtriser d'ici 2010. Ils ont également défini pour chacun des métiers les compétences nouvelles, non encore identifiées qu'il faudrait acquérir pour se préparer au changement à venir.

Ce document se décompose donc en trois parties. Une première partie est consacrée à un rappel méthodologique des différentes étapes constitutives de la démarche d'anticipation des compétences. Une seconde partie s'intéresse à la présentation des différentes hypothèses d'évolution sélectionnées pour le domaine de la Sécurité de l'Information et le plan d'actions associé pour s'y préparer ou y parvenir. Une troisième partie porte sur la présentation des compétences clés et nouvelles pour chacun des métiers traités.

Partie 1 : Méthodologie

La démarche prospective proposée a pour premier objectif d'anticiper les évolutions possibles de l'environnement des métiers étudiés au Luxembourg à 3-5 ans, et d'identifier des actions permettant soit de se préparer vis-à-vis du futur probable, soit d'agir pro activement pour la réalisation d'un futur souhaité.

Le second objectif de cette démarche est de détecter les futurs besoins en compétences des métiers sélectionnés d'ici 2010. En réponse à ces besoins les organismes de formation pourront être en mesure d'identifier les besoins du marché pour adapter au mieux leur offre de formation.

Pour cela, il est rappelé brièvement quelles sont les phases clés à partir desquelles il est possible de déployer la démarche d'anticipation. A ce titre, il est indiqué que l'expertise du Centre Henri Tudor repose sur une démarche composée de 3 étapes:

Etape 1 : Description du métier

Objectif : Formaliser le profil professionnel du métier

Démarche :

- Recherche d'informations sur les pratiques du métier en Europe
- Groupe de travail et/ou entretiens avec des « experts » métiers ayant une vision de l'exercice du métier pour élaborer le profil professionnel

Etape 2 : Evolution du métier

Objectif : Anticiper les facteurs clés de l'évolution du métier d'ici 3-5 ans.

Démarche : 3 séances de groupe de travail réunissant :

- Des experts ayant une vision de l'exercice du métier.
- Des managers opérationnels et des responsables du domaine de la Sécurité de l'Information.
- Des représentants d'organismes de formation, d'associations et de fédérations professionnelles.

Etape 3 : Anticipation des compétences

Objectif : Anticiper les compétences actuelles et nouvelles qui seront essentielles dans l'exercice du métier demain pour identifier les besoins/nécessités auxquels le métier sera confronté.

Démarche :

Une séance de groupe de travail réunissant le même type d'acteurs que l'étape 2.

Partie 2: Le profil d'évolution du domaine de la Sécurité de l'Information

1. Le Scénario d'évolution

Le scénario d'évolution est construit à partir des déterminants de l'évolution du métier étudié au Luxembourg d'ici 2010. Les déterminants identifiés sont de nature réglementaire, normative, technologique, économique, sociale, culturelle et organisationnelle, relevant d'un environnement national et international. Ces déterminants expliqueront demain l'évolution du métier sélectionné. Le tableau ci-dessous présente le scénario d'évolution, élaboré par le groupe de travail « Evolution de l'environnement du domaine de la Sécurité de l'Information ». Ce tableau expose à la fois les facteurs essentiels ainsi que les différentes hypothèses d'évolution qui ont été retenues pour analyser l'environnement des métiers sélectionnés.

Pour connaître les modalités d'élaboration du scénario d'évolution, un rapport documenté est disponible avec l'ensemble des étapes ayant permis sa construction. Il est téléchargeable sur le site : www.abilitic.eu

N°	Intitulés des facteurs essentiels d'évolution	Hypothèses d'évolution retenues
1	Absence d'une entité d'assistance (Computer Emergency Respons Team : CERT)	<i>En 2010 émergence d'une entité d'assistance (CERT) au Grand-duché du Luxembourg</i>
2	Sensibilisation par les pouvoirs publics et les associations aux risques en matière de Sécurité de l'information	<i>En 2010, les pouvoirs publics et les associations intensifieront la sensibilisation à la Sécurité de l'Information. (multiplication des cibles)</i>
3	Évolution des technologies (prise en compte des problématiques sécurité)	<i>En 2010, il y aura une prise en compte de la sécurité dès la phase de conception dans les technologies</i>
4	Assurer l'interopérabilité des technologies de la sécurité de l'information à développer, afin d'en améliorer la diffusion	<i>En 2010, en l'absence de normalisation, il n'y aura que des standards de fait qui s'imposeront via des technologies qui auront un certain degré de maturité</i>
5	Imposer la mise en place d'un niveau de sécurité minimum dans les entreprises	<i>En 2010, les autorités compétentes (administratives et/ou réglementaires) imposeront la mise en place d'un niveau de sécurité minimum et/ou certaines règles de sécurité aux entreprises de certains secteurs (exemple du secteur financier qui est un secteur régulé)</i>
6	Intégration du risk management à tous les niveaux de l'entreprise quelle que soit sa taille, son secteur d'activité	<i>En 2010 l'intégration du Risk Management sera plus homogène grâce à sa promotion et à la prise de conscience des entreprises</i>
7	Intégrer la sécurité dans le cadre d'une demande qualité	<i>En 2010, il y aura une convergence de la qualité et de la sécurité grâce à l'intégration de la sécurité dans les normes qualité. (ISO)</i>
8	Les Systèmes d'information et de communication (SIC), infrastructures critiques au même titre que l'eau et l'électricité	<i>En 2010, la criticité des Systèmes d'Information et de Communication sera de plus en plus importante au même titre que des ressources primaires (eau, électricité) : forte dépendance de la part des entreprises/organisations vis à vis des SIC</i>
9	Évolution brutale en cas de catastrophe numérique (11 septembre numérique)	<i>En 2010, l'impact d'éventuelles catastrophes numériques sera réduit grâce à une systématisation/amélioration de l'analyse des risques et de la gestion des crises. (multiplication des procédures et des tests de fiabilité des systèmes, redondance des moyens informatiques)</i>
10	Implication des Internet Service Provider (ISP) ou Fournisseurs d'Accès Internet (FAI) tout en respectant leur immunité	<i>En 2010 l'auto régulation du marché et la mise en place de codes de bonnes conduites va impliquer les ISP dans la sécurité de l'information</i>

2. Le plan d'action

Une fois, le scénario d'évolution identifié, le groupe de travail a proposé une série d'actions qui permettrait de se préparer ou parvenir à atteindre les évolutions envisagées. Les professionnels consultés ont mis en lumière les actions prioritaires. Celles-ci pourraient être diffusées auprès de l'ensemble des acteurs de la Sécurité de l'Information. Ces actions sont de couleur **bleue**. Des commentaires explicatifs supplémentaires justifient pour certaines, le choix des experts consultés.

En 2010, émergence d'une entité d'assistance (CERT) au Grand-duché du Luxembourg :

Au début de l'année 2007, les experts consultés ont envisagé la création d'un CERT national d'ici la fin de l'année. Cela se fera grâce à la volonté politique et les financements publics nécessaires. Ce CERT sera donc créé sous l'impulsion du gouvernement Grand Ducal. Jusqu'en 2010, le CERT s'attachera principalement à traiter des questions liées au Critical Infrastructure Protection (CIP). Au-delà de 2010, le CERT devra devenir selon les experts, l'interlocuteur privilégié des acteurs de la Sécurité de l'Information. Pour aboutir à cette perspective, les experts ont identifié plusieurs actions à mettre en œuvre :

- Imposer ou inciter la collaboration des entreprises avec le CERT afin que ces dernières communiquent des informations en lien avec des incidents relatifs à la Sécurité de l'Information

Les pouvoirs publics ont notamment besoin de récolter des informations pour les infrastructures critiques: énergie, transport, alimentation, télécommunications, santé, place financière.

- Garantir l'anonymat et la confidentialité des informations recueillies auprès des entreprises, ce qui facilitera leur volontariat.

Le volontariat des entreprises pour collaborer avec le CERT dépendra largement de la capacité de ce dernier à "gagner leur confiance". Plus cela sera effectif, plus le rôle du CERT sera reconnu par les professionnels de la Sécurité de l'Information. Les actions de diffusion, de veille sécurité, de sensibilisation à l'actualité des attaques I.T. et des scénarii de défense auront d'autant plus de pertinence.

- **Prévoir la mise en place d'échanges avec les CERT étrangers**

L'intérêt d'être en contact avec des CERT étrangers, est de pouvoir enrichir son travail de diffusion et de sensibilisation vis à vis des acteurs de la Sécurité de l'Information au Luxembourg

Le choix des experts s'est donc porté sur l'action en gras pour cette hypothèse d'évolution. Ils ont considéré que le CERT obtiendra sa légitimité avant tout par ce type d'action. Celle-ci leur paraît la plus pragmatique dans la mesure où cela va engendrer un échange d'information du CERT vers les entreprises luxembourgeoise. Il a même été suggéré d'acquiescer une renommée sur un secteur précis (le secteur financier par exemple) et obtenir cette légitimité également par rapport aux autres CERT étrangers.

Toutefois, les experts sont conscients que les PME luxembourgeoises sont certainement celles qui ont le plus besoin d'assistance en matière de Sécurité. Un arbitrage judicieux devra donc être fait.

En 2010, les pouvoirs publics et les associations intensifieront la sensibilisation à la Sécurité de l'Information. (Multiplication des cibles). Plusieurs actions sont proposées pour aller en ce sens :

- Intégrer les questions de Sécurité de l'Information dans toutes les formations professionnelles, voire même au niveau scolaire
- Promouvoir les certifications du type e-privacy, e-commerce certified
- **Sensibiliser la société aux risques en matière de Sécurité, à la criminalité informatique, ainsi qu'aux conséquences (juridiques, notamment) des actes de malveillance dans ce domaine**

L'action prioritaire en gras insiste sur le fait de sensibiliser sur les risques en matière de Sécurité. Cela devrait permettre selon les experts de toucher directement ou indirectement les PME luxembourgeoises qui sont à nouveau, apparues comme une cible critique.

En 2010, il y aura une prise en compte de la sécurité dès la phase de conception dans les technologies. Pour suivre cette évolution, les experts du Groupe de Travail ont envisagé :

- Accroître la sensibilisation à l'intégration des questions de Sécurité de l'Information dans les technologies
- **Elaborer des standards de sécurité pour le début et tout au long des cycles de développement des technologies**
- Proposer des formations en sécurité aux personnes chargées du développement des technologies et/ou systèmes

Ainsi, dès l'élaboration du cahier des charges d'une nouvelle technologie, les experts espèrent qu'il y aura une identification et une prise en compte systématique des risques en matière de Sécurité de l'Information

Les experts insistent en terme d'action prioritaire sur celle en gras. Ils prennent pour exemple le cas de l'entreprise de Microsoft qui a commencé à intégrer cette évolution. Pour appuyer cette action, les experts estiment nécessaire d'avoir le soutien de département Marketing au sein des entreprises qui vendent des technologies. Ces derniers sont en effet sensibles aux conséquences commerciales suite à des accidents dus à une non prise en compte des questions de Sécurité.

En 2010, en l'absence de normalisation, il n'y aura que des standards de fait qui s'imposeront via des technologies qui auront un certain degré de maturité. Les experts préconisent les actions suivantes:

- **Promouvoir l'usage des standards et des normes en matière d'interopérabilité pour les moyens IT choisis et mis en oeuvre**
- Sensibiliser les acteurs majeurs de l'industrie (clients et surtout les fournisseurs) sur la nécessité de l'interopérabilité

En 2010, les autorités compétentes (administratives et/ou réglementaires) imposeront la mise en place d'un niveau de sécurité minimum et/ou certaines règles de sécurité aux entreprises de certains secteurs (exemple du secteur financier qui est un secteur régulé). Les actions suivantes ont été suggérées :

- Promouvoir et inciter l'application de telles dispositions réglementaires
- Il est notamment préconisé par les experts d'élaborer des argumentaires devant mettre en avant les gains de compétitivité de l'application de telles dispositions réglementaires. Cela faciliterait l'appropriation et la compréhension de ces dispositions réglementaires
- **Sensibiliser le législateur aux pratiques de certaines entreprises qui ont des activités critiques et qui ont généré des standards de fait pour en faire pourquoi pas des prescriptions à respecter.**
 - Faire suivre l'évolution des normes internationales pour imposer/inciter la mise en place d'un niveau minimum de sécurité

En 2010 l'intégration du Risk Management sera plus homogène grâce à sa promotion et à la prise de conscience des entreprises. En d'autres termes, les pratiques d'intégration du Risk Management seront mieux harmonisées parmi toutes les entreprises. Il en découlera une professionnalisation croissante de l'organisation des entreprises. Aussi, pour y parvenir, les experts envisagent de :

- Promouvoir des formations liées à l'intégration du Risk Management dans les pratiques des entreprises
- **Imposer pour certains secteurs, secteur régulé notamment, la mise en place du Risk Management et certains modes de gestion du Risk Management**

Il est pressenti par ailleurs que "l'amont de la chaîne économique", c'est-à-dire les entreprises ou les organisations influentes sur le marché vont imposer l'intégration de règles spécifiques en Risk Management aux sous traitants. Cela aura pour conséquence de promouvoir des standards spécifiques.

Les experts ont donc mis en évidence l'action en gras au regard de ce qui existe déjà actuellement. La CSSF devrait en effet préconiser si ce n'est déjà fait une telle orientation. Dans tous les cas, les éléments présents dans cette étude peuvent permettre d'appuyer encore davantage la nécessité de s'orienter vers de telles pratiques.

En 2010, il y aura une convergence de la qualité et de la sécurité grâce à l'intégration de la sécurité dans les normes qualité. (ISO). Pour parvenir à cette évolution, les experts estiment judicieux notamment de :

- Participer aux activités de normalisation et préconiser la certification sur les standards de sécurité et de qualité pour des activités clés au sein des organisations.
- **Favoriser dans ce cadre, le développement de la sécurité dans les normes ISO via le SC (sous-comité) 27 du « consortium » ISO auquel le Luxembourg participe.**

Cela permettra de défendre ainsi le point de vue Grand Ducal lors de l'évolution des normes et des votes d'adoption.

En 2010, la criticité des Systèmes d'Information et de Communication sera de plus en plus importante au même titre que des ressources primaires (eau, électricité) : forte dépendance de la part des entreprises/organisations vis à vis des SIC. Pour se préparer à cette évolution, les experts proposent les actions suivantes :

- Assurer la sécurité physique des infrastructures par la création de sites secondaires, de systèmes redondants.
- **Mettre en place des contrôles systématiques notamment sur l'état des systèmes tels que ceux liés au monitoring ou encore sur l'intégration des exigences de Qualité.**

La recherche de certification via la norme ISO 27001 par exemple représenterait une action de préconisation parmi d'autres pour prendre en compte le caractère critique des Systèmes d'Information de Communication

En 2010, l'impact d'éventuelles catastrophes numériques sera réduit grâce à une systématisation/amélioration de l'analyse des risques et de la gestion des crises. (Multiplication des procédures et des tests de fiabilité des systèmes, redondance des moyens informatiques). Les experts préconisent pour parvenir à cette évolution de :

- Harmoniser les approches dites d'analyse des risques ainsi que du vocabulaire employé.
- **Réaliser un état des lieux national au niveau des pratiques en matière de Sécurité de l'Information, étude devant de préférence être effectuée par le Haut Commissariat à la Protection Nationale.**

Cette étude pourrait présenter un recensement des incidents, des menaces, vulnérabilités, probabilités, et impacts que ces derniers peuvent avoir sur les entreprises du Grand-duché. Une attitude attentiste consisterait à attendre une réelle catastrophe numérique de grande ampleur. Les acteurs de la Sécurité de l'Information prendraient alors certainement consciences de l'intérêt de porter un regard critique sur les pratiques d'analyse et de gestion des crises.

- Engager une réflexion pour définir comment diffuser au mieux les résultats des études précédentes aux acteurs concernés.

Ces réflexions devraient permettre d'aboutir :

- à l'identification des acteurs, des opérateurs d'infrastructures critiques à joindre en cas de crise : avec la mise en place d'un Business continuity plan (BCP) au niveau national
- à l'identification des services primordiaux à mettre en place prioritairement (procédures BCP) au sein des organisations mêmes (idée de "mettre en réserve" pour pouvoir relancer la machine, l'entreprise)

En 2010 l'auto régulation du marché et la mise en place de codes de bonnes conduites va impliquer les ISP dans la sécurité de l'information. Pour permettre cette évolution, les experts distinguent plusieurs actions :

- Inciter les ISP à être plus regardant sur le contenu et la nature des échanges effectués par les internautes via les services qu'ils proposent.

Cette incitation pourra ou devra venir, soit de l'opinion publique, soit suite à l'intervention de l'Institut Luxembourgeois de Régulation (IRL) ou encore des organisations représentatives telles que l'Internet Service Provider Association (ISPA), L'Association des Professionnels de la Société de l'Information (APSI), voire même peut-être des pouvoirs publics.

- **Reconsidérer le statut des ISP pour leur permettre de collaborer au mieux à des bonnes pratiques en matière de Sécurité de l'Information.**

La divulgation des informations confidentielles détenues par les ISP ne pourrait s'envisager sérieusement qu'à travers un cadre législatif européen. Ce qui n'est pas le cas aujourd'hui. Il apparaît nécessaire selon les experts de procéder à une évolution de contenu du cadre législatif national et/ou communautaire en lien avec ces éléments.

Les experts ont considéré l'action en gras comme prioritaire dans la mesure où ils y voient la possibilité de pouvoir solliciter les ISP pour des incidents ayant des impacts critiques pour une entreprise, un secteur d'activité, etc. Ils émettent l'hypothèse via cette action de pouvoir indirectement responsabiliser les ISP sur leur rôle en matière de bonnes conduites à tenir.

L'impact des hypothèses d'évolution sur les référentiels de compétences est présenté ci après. Cela permet d'identifier les compétences clés des métiers sélectionnés à horizon 2010 et d'envisager quels sont les éléments nouveaux à intégrer en terme de compétences pour ces métiers.

Partie 3 : L'identification des compétences clés et nouvelles des métiers étudiés

Le développement qui suit se décompose en plusieurs parties. La première partie fait un rappel de la structure utilisée pour décrire les métiers étudiés ainsi que de la finalité des différents exercices qui ont été proposés durant les précédents Groupes de Travail de l'année 2007. La seconde partie s'attache quant à elle, pour chacun des métiers, à exposer les différents outputs de la démarche d'anticipation qui résulte des différents exercices d'évaluation. Ainsi, l'impact des changements clés à horizon 2010 du domaine de la Sécurité de l'Information sur le profil professionnel sera mis en avant pour chaque métier. L'identification des compétences clés et des compétences nouvelles qui en découle, sera également présentée.

1. Rappel :

A. La structure des profils professionnels

Le profil professionnel décrit le travail que les professionnels accomplissent dans le cadre de leur métier ou de leur profession. Les métiers étudiés sont présentés en termes **d'activités, de tâches et de compétences**. L'idée à travers cette structuration est d'exprimer un niveau de granularité de plus en plus fin dans les expressions utilisées.

- En effet, le métier est tout d'abord découpé en **activités**. Ces activités correspondent à des blocs thématiques, des prérogatives qui sont de la responsabilité du métier étudié. Une activité comprend dans le cadre du profil professionnel un ensemble d'actions visant à l'accomplissement d'un travail déterminé.
- Ces activités sont ensuite déclinées en plusieurs **tâches**. Ces dernières sont par conséquent appréhendées comme des subdivisions de l'activité, c'est-à-dire une action réalisée dans le cadre de l'activité.
- Enfin, la notion de **compétence** est définie comme un ensemble de savoirs, savoir-faire, savoir-être et savoirs technologiques à mettre en œuvre pour accomplir une tâche. Les savoirs et savoirs technologiques sont formulés par des expressions nominatives, les savoir-être par des qualificatifs, et les savoir-faire correspondent à des actions précises à réaliser.

Pour chaque métier, il s'agit de la vision des métiers à partir de laquelle les parties prenantes du projet (CRP Henri Tudor, représentants institutionnels du domaine de la Sécurité de l'Information, experts sollicités) ont souhaité travailler.

B. L'impact du scénario d'évolution sur le profil professionnel des métiers de la Sécurité de l'Information

Il s'agit ici de mesurer l'impact des changements décrits par le scénario d'évolution sur chacun des profils professionnels des métiers choisis dans le cadre de la démarche d'anticipation. Le but est de sélectionner les tâches les plus impactées par le changement.

C. L'identification des compétences clés et nouvelles des quatre métiers étudiés pour le domaine de la Sécurité de l'Information

Les compétences essentielles à la mise en œuvre des tâches les plus impactées par le changement constituent les compétences clés. Il a donc été demandé aux experts de les identifier. Cela a donc permis d'aboutir à la détection des compétences actuelles qui seront essentielles dans l'exercice des métiers sélectionnés à l'horizon 2010.

Par ailleurs, le profil professionnel n'étant pas exhaustif, une réflexion pour chacun des métiers a été proposée pendant les Groupes de Travail pour permettre l'identification des compétences nouvelles à horizon 2010.

2. Les résultats

Pour chaque métier, un rappel des missions génériques attribuées au métier sera fait. Par la suite, la mesure de l'impact du scénario d'évolution du domaine de la Sécurité de l'Information ainsi que l'identification des compétences clés et nouvelles à horizon 2010 seront mis en avant à partir du descriptif des activités, tâches et compétences de chacun des métiers,

- Les tâches du métier qui ont été impactés par le scénario d'évolution sont signalées par la couleur **Bleue**.
- Les compétences clés sont matérialisées par la même signalétique que les tâches
- Les compétences nouvelles sont quant à elles regroupées dans un tableau de synthèse qui recueille les propos exprimés par les experts sollicités dans les groupes de travail organisés durant l'année 2007.

A. Pour le métier d'Auditeur en Sécurité de l'Information

Missions : Le rôle de l'auditeur en Sécurité de l'information est de remplir, à la demande, des missions spécifiques de vérification de l'existant, au cœur d'une organisation, en conformité avec un référentiel déterminé pour la Sécurité de l'Information.

L'impact du scénario d'évolution sur les tâches et compétences du métier :

Les activités principales et tâches associées

<p style="text-align: center;">Contextualiser la mission d'audit</p> <ul style="list-style-type: none"> ○ Mettre à jour ses connaissances pour la réalisation de l'audit ○ Analyser le scope de la mission ○ Etablir le budget et définir les compétences correspondantes nécessaires à la mission d'audit ○ Structurer la gestion de projet de l'audit ○ Clôturer la préparation de la mission 	<p style="text-align: center;">Dérouler la mission d'audit</p> <ul style="list-style-type: none"> ○ Réaliser des interviews et des entretiens ○ Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre) ○ Documenter la réalisation de l'audit ○ S'assurer du bon déroulement des étapes du projet (RH, disponibilités) ○ Identifier les forces et faiblesses du périmètre d'analyse et du référentiel ○ Valider les faits (forces et faiblesses)
<p style="text-align: center;">Orchestrer et développer la communication envers le(s) commanditaire(s) de l'audit et les audités</p> <ul style="list-style-type: none"> ○ Présentation de la validation des faits aux commanditaires ○ Etablir le rapport d'audit ○ Intégrer les commentaires des audités ou commanditaires ○ Proposer un questionnaire de satisfaction par rapport aux pratiques de l'équipe audit ○ Rendre compréhensible et synthétique le rapport détaillé de l'audit pour le top management et l'organe de tutelle 	<p style="text-align: center;">Manager une équipe d'audit</p> <ul style="list-style-type: none"> ○ Gérer les compétences, personnalités, attentes, contraintes, etc, de l'équipe ○ Organiser et suivre le travail des auditeurs ○ Evaluer le travail de l'équipe ○ Standardiser les méthodes de travail (approche commune) ○ Gérer le tableau de bord des audités
<p style="text-align: center;">S'intégrer dans une équipe d'audit</p> <ul style="list-style-type: none"> ○ Comprendre le contexte de l'équipe d'audit ○ Comprendre ses contraintes en tant qu'auditeur ○ Communiquer avec sa hiérarchie ○ Communiquer avec les autres fonctions de contrôle 	

[en gras les tâches les plus impactées par les hypothèses d'évolution]

Les compétences de l'Auditeur en Sécurité de l'Information

Savoirs	Savoir-être
<p>Savoirs clés :</p> <ul style="list-style-type: none"> ○ Processus business ○ Méthodes de gestion et d'analyse des risques (Ebios, Mehari, Marion, Calio, Melisa, Cramm, Octave, etc) ○ Normes professionnelles de l'audit (IA, ISACA) ○ Normes et procédures de sécurité IT ○ Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001) ○ Techniques d'entretiens propres à l'audit ○ Charte d'utilisation et de sécurité des Systèmes d'Information ○ Concepts et pratiques d'audit ○ Environnement de l'entreprise ○ Fonctionnement des organisations ○ Gestion et conduite de projets ○ Gestion des compétences ○ Gestion des conflits ○ Règles et pratiques juridiques en matière de protection de la propriété intellectuelle, copyright, protection des données, etc ○ Stratégie d'entreprise ○ Théorie et application de la cryptologie 	<p>Savoir-être clés :</p> <p>Aucun des savoir-être ci-après n'a été identifié comme clés à horizon 2010</p> <ul style="list-style-type: none"> ○ Analyste pour interpréter le recueil d'informations suite aux différentes interviews ○ Diplomate - Aisance relationnelle afin de pouvoir obtenir les informations nécessaires à la réalisation de l'audit, et de restituer de manière appropriée les informations liées à son travail ○ Discret dans la manière de recueillir les informations et de ne pas les divulguer ○ Disponible par rapport aux exigences et aux contraintes organisationnelles de l'entreprise auditée ○ Indépendant dans la manière de dérouler les différents entretiens pour réaliser un audit, dans la manière de produire les documents nécessaires au rapport d'audit ○ Intègre dans la manière d'analyser et de restituer l'information sans à priori, ni préjugés ○ Leadership dans le cas où l'auditeur serait amené à manager une équipe ○ Ouvert d'esprit pour être réceptif aux différentes configurations organisationnelles existantes, pour être à jour sur les évolutions technologiques en matière de sécurisation des Systèmes d'Information et de Communication ○ Rigoureux pour s'appliquer à vérifier la conformité aux exigences du référentiel ○ Travailler en équipe pour évoluer avec des personnes supports, avec les représentants de l'entreprise et/ou du département audité
<p style="text-align: center;">Savoir-faire</p> <p>Savoir-faire clés :</p> <ul style="list-style-type: none"> ○ Analyser de l'information technique et organisationnelle (revue de procédures internes, historique de l'entreprise) ○ Identifier et prendre en compte des données stratégiques de l'entreprise ○ Définir l'objectif et le programme d'audit correspondant, (re) définir des missions, des fonctions et des actions pour les différents acteurs de l'entreprise ○ Elaborer un questionnaire d'audit ○ Dialoguer - interroger - interviewer des collaborateurs ○ Effectuer la collecte des données et l'agrégation des données ○ Faire un audit de l'architecture réseau, des procédures d'exploitation, des procédures organisationnelles, du logiciel serveur, du matériel, des services (climatisation, onduleur par ex) ○ Mettre en place des indicateurs afin de s'assurer de l'application de normes et standards ○ Réaliser et/ou valider des rapports d'audit, des rapports de non-conformité, des rapports d'actions correctives et préventives, et des supports d'informations sur le déroulement de l'audit ○ Se tenir informé des évolutions réglementaires, du référentiel de base, des normes, standards et du contexte de l'entreprise. ○ Tenir à jour les templates communs d'audit ○ Rédiger ou participer à la rédaction d'une lettre de mission ○ Faire évoluer le questionnaire d'Audit ○ Effectuer des réunions d'ouverture et de clôture d'audit ○ Demander l'accès aux documents pertinents ○ Mettre en œuvre une analyse des risques ○ Planifier et ordonnancer des audits ○ Valider des constats d'action avec le ou les responsables de l'entité auditée ○ Alerter la hiérarchie en cas de problèmes majeurs ○ Se soucier de la qualité de service au client 	<p style="text-align: center;">Savoirs technologiques</p> <p>Savoir technologique clé :</p> <ul style="list-style-type: none"> ○ Intégration de nouvelles technologies au SI ○ Architecture fonctionnelle du SI (Système d'Information) de l'entreprise (logiciels, applications métiers) ○ Environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données...) ○ Architecture de systèmes d'exploitation ○ Architecture des réseaux informatiques et télécoms ○ Architecture technique du SI de l'entreprise ○ Intégration de systèmes d'exploitation ○ Droits d'accès aux applications et services ○ Développement d'algorithmique ○ Protocoles de communication

Les compétences nouvelles pour l'Auditeur en Sécurité de l'Information

Orientation de la pratique du métier	<p>La pratique des audits se fait aujourd'hui dans un cadre temporel relativement "long" et ponctuel. A l'avenir il semblerait que la pratique de l'audit en Sécurité de l'Information se fera davantage dans un cycle court et continue afin d'être systématisé et probablement aussi pour pouvoir comparer des résultats successifs et mesurer les évaluations. Cela accentuera les exigences demandées en terme de délais/qualité pour réaliser les Audits en Sécurité de l'Information.</p> <p>Il y aura également un accroissement (intensification) du besoin de connaissances des systèmes d'évaluation et de certifications internationaux</p> <p>A terme, une catégorisation des audits serait exigée pour permettre de répondre au mieux aux nouvelles exigences du marché, ce qui pourrait impliquer que d'ici 2010 les auditeurs se spécialisent sur des normes, des référentiels, des éléments techniques ou organisationnels en lien bien entendu avec des problématiques relatives à la Sécurité de l'Information</p>	
Types de compétences	Éléments nouveaux exprimés par les experts	Commentaires explicatifs
Savoir	Augmenter ses connaissances des lois liées à la protection de la vie privée (données personnelles) dans la sphère professionnelle	<p>Il semblerait que le métier d'Auditeur en Sécurité de l'Information, de part l'évolution des technologies qui pourront aller toujours plus loin dans la manière de contrôler/vérifier les pratiques de leurs salariés, devra être en mesure de s'assurer que les pratiques mis en oeuvre pour relever les preuves et les évidences seront toujours en règle par rapport aux éléments législatifs liés à la protection de la vie privée, à la protection des données.</p> <p>Le développement du télé - travail devrait également dans ce cadre impacter les pratiques de l'Auditeur en Sécurité de l'Information. Ce mode de fonctionnement implique de nombreuses modifications au niveau du respect des pratiques énoncées par l'entreprise en matière de Sécurité de l'Information. Ces modifications de pratiques de travail devront s'inscrire au regard d'éléments normatifs tel que la norme ISO 27001</p>
Savoir - Faire	<p>Élaborer des outils, des dispositifs de veille pour la mise à jour de ses connaissances, notamment pour les connaissances nécessaires aux processus de certification appliqués à la Sécurité de l'Information</p> <p>Intégrer l'évaluation du risque de sécurisation de l'Information en fonction de l'adéquation entre RH et responsabilités/tâches allouées</p> <p>Identifier les bons interlocuteurs (en matière de compétences, de positionnement dans l'organisation) pour se faire accompagner de façon significative dans le déroulement de l'Audit</p> <p>S'assurer de la cohérence/pertinence du programme d'audit au regard du contexte d'utilisation de ce dernier (contextualisation de l'analyse des risques)</p> <p>Évaluer/estimer de manière plus fine le temps adéquat pour la réalisation/ le déroulement du programme d'audit et en dresser le programme</p>	<p>Lors des phases de contextualisation et de déroulement de l'Audit, un focus plus important devrait être porté sur le facteur humain. Actuellement, la prise en compte des aspects techniques est prépondérante, il n'y a pas de prise en compte des vulnérabilités humaines et des conséquences que cela peut impliquer pour l'organisation au niveau de la sécurisation de l'Information</p> <p>L'auditeur devra être attentif aux personnes qu'ils sollicitent au sein de l'organisation pour déployer son audit, au delà de celles qui sont interviewées/interrogées dans le cadre du programme d'audit</p> <p>Un accompagnement de l'Auditeur, notamment au niveau juridique apparaîtrait de plus en plus nécessaire au regard de la complexification des dispositifs réglementaires en matière de sécurisation de l'information</p> <p>Cela passe par la définition de critères de qualité minimum (procédure, check liste, méthodologies) dans l'exécution de programme d'audit afin d'éviter les dérives de sous - évaluation du temps nécessaire affecter à la réalisation de l'audit. Cet élément est à mettre en relation avec la pression croissante (tendance) exercée sur les auditeurs pour réaliser des audits avec des cycles plus courts et répétitifs</p>
Savoir - être	<p>Faire respecter son intégrité dans le déroulement et l'analyse de son travail (que l'Auditeur soit en interne ou en externe)</p> <p>Savoir évoluer dans une logique de co construction entre junior et senior</p>	<p>La chartre déontologique de l'Auditeur en Sécurité de l'information subira de plus en plus de pression à horizon 2010 au regard des éléments cités précédemment</p> <p>Le souci du transfert de connaissances entre auditeur senior et junior ou entre auditeur d'un même niveau travaillant sur une même mission est apparue clé pour l'évolution du métier. Les auditeurs devraient davantage s'inscrire dans une logique de co - construction, c'est à dire s'inscrire dans une logique d'échanges de bonnes pratiques pour permettre un déploiement des audits plus homogènes, au delà de l'homogénéisation des méthodes</p>
Savoir - technologique	Connaissance, capacité accrue d'identification des flux d'informations liés au fonctionnement d'un "système d'information"	Cette connaissance apparaît judicieuse pour appréhender au mieux les mécanismes de fonctionnement de logiciels qui fonctionnent notamment à l'insu des utilisateurs

B. Pour le métier de Consultant en Sécurité de l'Information

Missions : La mission du consultant en Sécurité de l'Information est de répondre aux besoins définis en proposant des solutions adaptées aux clients souhaitant mettre en place, modifier, ou renouveler leur stratégie et/ou pratiques opérationnels en matière de Sécurité de l'information au sein d'une organisation.

L'impact du scénario d'évolution sur les tâches et compétences du métier :

Les activités principales et tâches associées

<p>Prendre en charge les enjeux et les spécificités du client</p> <ul style="list-style-type: none"> ○ Prendre connaissance de l'existant ○ Comprendre les spécificités du client ○ Comprendre le fonctionnement interne de l'entreprise ○ Analyser les besoins ○ Traduire les spécificités fonctionnelles et non fonctionnelles en plans d'action, en politique de sécurité, etc ○ Assurer un pilotage stratégique 	<p>Collaborer au développement de la prestation en assistant la Maîtrise d'Ouvrage (MOA) et la Maîtrise d'œuvre (MOE)</p> <ul style="list-style-type: none"> ○ Formaliser l'analyse de l'existant ○ Formaliser les conclusions de l'analyse ○ Assurer l'adéquation entre les recommandations proposées et la mise en oeuvre des solutions ○ Participer à l'élaboration d'un cahier des charges ○ Etudier les intégrateurs, les distributeurs et les solutions du marché ○ Evaluer les solutions proposées ○ Participer à l'élaboration de l'expression des besoins ○ Négocier si besoin à la contractualisation de la relation MOA/MOE ○ Valider les livrables (recettes)
<p>Accompagner l'aide au changement par des actions de communication et de formation</p> <ul style="list-style-type: none"> ○ Encadrer le client dans son apprentissage des enjeux liés à la Sécurité de l'Information ○ Définir et appliquer le schéma de communication en lien avec la ou les solutions proposées ○ Personnaliser son langage en fonction des collaborateurs rencontrés ○ Se former aux évolutions du domaine de la Sécurité de l'Information et aux pratiques et stratégies des entreprises 	

[en gras les tâches les plus impactées par les hypothèses d'évolution]

Les compétences du consultant en sécurité de l'information

Savoirs	Savoir-être
<p>Savoirs clés :</p> <ul style="list-style-type: none"> ○ Fonctionnement des organisations ○ Gestion du changement ○ Gestion et conduite de projet ○ Méthodes de gestion et analyse des risques (Ebios, Mehari, Marion, Melisa, Cramm, Octave) ○ Normes professionnelles d'audit (IA, ISACA, etc) ○ Normes et procédures de sécurité IT ○ Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001) ○ Processus business ○ Stratégie d'entreprise ○ Veille technologique ○ Environnement de l'entreprise ○ Concepts et pratiques d'audit ○ Techniques d'entretiens ○ Stratégie commerciale ○ Contexte des impératifs et mobiles commerciaux des prestataires ○ Gestion des compétences ○ Règles et pratiques juridiques en matière de protection des données, protection de la propriété intellectuelle, copyright ○ Politique de sécurité ○ Charte d'utilisation et de sécurité SI 	<p>Savoir-être clés :</p> <ul style="list-style-type: none"> ○ Aisance relationnelle afin de pouvoir recueillir les informations nécessaires à la prestation, et de dialoguer avec l'ensemble des personnes qui pourraient être impactées par les résultats de sa prestation ○ Ouvert d'esprit pour être réceptif aux différentes configurations organisationnelles existantes, pour être à jour sur les évolutions technologiques en matière de sécurisation des SIC ○ Rigoureux pour mener à bien l'intégralité de la prestation ○ Intègre : dans la manière de proposer des solutions qui correspondent aux besoins du projet ou aux exigences du client ○ Autonome dans la manière de dérouler la prestation, dans la manière de proposer l'état comparatif des meilleures solutions envisagées, dans la manière de réaliser tout ou partie du développement demandé ○ Disponible par rapport aux exigences et aux contraintes organisationnelles de l'entreprise dans laquelle il est amené à prester un service ○ Travailler en équipe pour évoluer avec des personnes supports, avec les représentants de l'entreprise et/ou du département demandeuse ○ Négociateur – Persuasif dans les phases de contractualisation avec le client, dans les phases de discussion pour le choix d'une solution, dans les différents échanges devant faciliter l'acceptation des solutions envisagées. ○ Proactif dans la mesure où il se doit de suivre les évolutions technologiques, réglementaires de son domaine et proposer parallèlement à cela des prestations adéquates à ses clients ○ Analyste pour comprendre l'organisation dans laquelle il est amené à travailler et identifier ses besoins et ses contraintes
<p>Savoir-Faire</p> <p>Savoir-Faire clés :</p> <ul style="list-style-type: none"> ○ Analyser l'existant (revue de procédures internes, historique de l'entreprise) ○ Animer et préparer des réunions ○ Connaître l'environnement technique et comprendre les solutions proposées à travers le langage commercial ○ Effectuer une veille concurrentielle ○ Identifier la taille, la nature et la complexité de l'organisation analysée ○ Identifier les besoins en connaissances du client ○ Mettre en conformité l'organisation ○ Réaliser un diagnostic des besoins ○ Réaliser des études d'impact, des études de marchés (fournisseurs) ○ Valider une solution informatique ou organisationnelle en Sécurité ○ Savoir s'adapter à différents types d'interlocuteurs ○ Respecter la « déontologie » de la fonction de consultant ○ Traduire des non - conformités en solution pour le développement de la sécurité de l'Information ○ Prendre en compte des données stratégiques de l'entreprise ○ Sonder des collaborateurs ○ Effectuer la collecte et l'agrégation des données ○ Rédiger le cahier des charges et le cahier fonctionnel ○ Définir l'objectif de la prestation ○ Co-rédiger les appels d'offres ○ Étudier les solutions logicielles et/ou applicatives existantes en matière de Sécurité de l'Information ○ Soutenir la prise de décision du client dans ses décisions ○ Planifier un plan d'actions ○ Rédiger des architectures sécurité- réseaux ○ Conseiller des programmes anti-intrusions ○ Réaliser des tests techniques ○ Vérifier les potentialités du système ○ Identifier les bugs de logiciels éventuels ○ S'assurer des bonnes pratiques de maintenance de ce système ○ Participer à la rédaction des scénarios et des cahiers de recette ○ Réaliser l'évaluation d'une situation, d'un état d'avancement ○ Participer à la présentation des maquettes des écrans ○ Mobiliser les connaissances liées aux savoirs technologiques en fonction du contexte de la mission 	<p>Savoirs technologiques</p> <p>Savoirs technologiques clés :</p> <ul style="list-style-type: none"> ○ Architecture des réseaux informatiques et télécoms ○ Environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données...) ○ Intégration de nouvelles technologies au SI ○ Architecture fonctionnelle du SI (Système d'information) de l'entreprise (logiciels, applications métiers) ○ Architecture technique du SI de l'entreprise ○ Solutions logicielles et/ou applications en matière de Sécurité de l'Information

Les compétences nouvelles pour le consultant en sécurité de l'information

Orientation de la pratique du métier	<p>A l'avenir, le Consultant en Sécurité de l'Information aura un rôle d'interface (encore) plus important entre les différents interlocuteurs qu'il est amené à rencontrer en entreprise, ou dans les organisations. Il devra être en mesure d'aligner au mieux les besoins de sécurité de l'organisation avec les solutions de sécurité proposées (réflexions et justifications mieux argumentées et structurées).</p> <p>Il se peut qu'à terme, deux profils de consultant apparaissent en Sécurité de l'Information. Il y aurait ainsi d'une part des professionnels spécialisés "sur" tous les aspects techniques liés à la Sécurisation de l'Information au sein d'une entreprise. D'autre part, il y aurait aussi des consultants, avec un bagage professionnel plus conséquent qui se spécialiseraient davantage sur des problématiques de Sécurisation de l'Information à un niveau organisationnel.</p> <p>Quel que soit le profil, le consultant devra de toute manière faire en sorte d'intégrer, de prendre en compte (encore davantage que cela n'est fait) les aspects/contraintes business de l'organisation pour laquelle il travaille. La question de la Sécurisation de l'Information doit s'adapter au Business et non l'inverse.</p>	
Types de compétences	Éléments nouveaux exprimés par les experts	Commentaires explicatifs
Savoir - Faire	Diriger et animer des réunions de travail, groupes de travail, débats d'experts de manières structurées et formelles.	Pour réussir les missions qui lui seront confiées, il devra être en mesure de fédérer différents interlocuteurs autour d'une ou de plusieurs problématiques posées par l'organisation. Il devra animer des réunions, de groupes de travail. Cette compétence ne sera plus périphérique à son cœur de métier. Elle composera son cœur de compétences au même titre que celles liées à l'analyse de l'existant ou encore à sa connaissance des éléments normatifs du domaine de la Sécurité de l'Information
	Elaborer et déployer des plans d'actions de sensibilisation des entreprises, salariés, aux enjeux et problématiques liés à la thématique de la Sécurité de l'Information	La sensibilisation apparaît être un point critique pour le métier de Consultant en Sécurité de l'Information. Cette pratique peut lui permettre d'être une porte d'entrée au sein des entreprises. Qui plus est, au delà d'une éventuelle démarche d'approche client, la pratique de sensibilisation doit être intégrée et s'inscrire en continu tout au long d'une prestation au sein d'une organisation.
	Suivre, identifier et évaluer les pratiques existantes en matière de Sécurisation de l'Information sur le marché afin de mesurer leur impact ou apport sur son propre business	Il devra être à l'écoute des nouveautés proposées sur le marché afin d'en déterminer la criticité pour sa propre activité. Si tel est le cas, il devra être en mesure de pouvoir se les approprier (acquisition de connaissances, compétences)
	Elaborer des pratiques de veille structurées pour suivre les évolutions réglementaires et normatives (tant au niveau local, régional, national, et international)	Il s'agit d'appréhender au mieux leurs impacts et contraintes par rapport au traitement de la question de la Sécurité de l'Information en organisation
	S'assurer de l'alignement des préconisations, solutions proposées avec la stratégie business de l'entreprise demandeuse	Que son intervention se situe à un niveau technique et/ou organisationnel, le Consultant en Sécurité de l'Information devra apprécier si ses préconisations/actions sont alignées avec la stratégie d'entreprise ou l'impact que cela peut avoir sur la stratégie d'entreprise.
	Garantir la bonne tenue du scope de la mission initiale avant tout élargissement potentiel de la prestation	Cela passe par une meilleure connaissance et maîtrise de la gestion des "effets de seuils" des missions prestées
Savoir - être	pédagogue	Il s'agit de démystifier les politiques de Sécurité auprès des opérationnels. Le consultant doit jouer un rôle éducatif en transposant le jargon professionnel vers l'utilisateur. Le but est d'ajouter à la solution technique un mode d'emploi et une adhésion immédiate et adaptée

C. Pour le métier d'Ingénieur - Chargé de monitoring des incidents IT

Missions : Le chargé de monitoring des incidents IT doit signaler les incidents IT identifiés en filtrant et interprétant les informations données par tous les outils de monitoring mis en place.

L'impact du scénario d'évolution sur les tâches et compétences du métier :

Les activités principales et tâches associées

<p>Identifier et traiter des incidents IT</p> <ul style="list-style-type: none"> ○ Détecter un incident à l'aide d'informations de tiers (client), d'outils/méthodes/systèmes d'observation et de prévention (logs, IPS², IDS³, corrélation d'évènements, etc) ○ Identifier et évaluer l'incident (nature, source, gravité, etc) ○ S'assurer que les objectifs de la politique sécurité sont transformés en éléments « identifiables et mesurables » dans le cadre de l'utilisation des outils de monitoring 	<p>Optimiser le système de monitoring des incidents IT</p> <ul style="list-style-type: none"> ○ Adapter les outils/méthodes/systèmes d'observation et de prévention ○ S'assurer de la fiabilité et du fonctionnement de son système (ex : par l'exécution de tests ciblés, etc) ○ Participer à l'élaboration du cahier des charges des besoins en monitoring et des besoins en outils de monitoring ○ Evaluer et si besoin modifier en accord avec sa hiérarchie, le processus de gestion et de traitement des incidents ○ S'assurer du maintien du niveau des objectifs sécurité en fonction des éléments « identifiables et mesurables »
<p>Participer à la communication et à la sensibilisation des commanditaires et/ou utilisateurs face aux incidents IT</p> <ul style="list-style-type: none"> ○ Participer à l'élaboration de la charte informatique à destination des utilisateurs ○ Rapporter l'incident à sa hiérarchie, à un CERT⁴, à ses clients/abonnés, à toute personne concernée par l'incident ○ Participer à la mise à jour des procédures ou pratiques liées à l'utilisation des outils IT ○ Compiler et organiser la documentation des incidents IT recensés (ainsi que les personnes ressources pour les traiter) ○ Collaborer (si besoin) à la réalisation des modules de formation et des manuels didactiques pour les utilisateurs 	<p>Participer à la mise en œuvre d'actions correctives</p> <ul style="list-style-type: none"> ○ Participer à la mise en place de mécanismes appropriés avec les personnes compétentes afin de minimiser les impacts/dommages/risques ○ Améliorer/Informer sur les possibilités de solutions alternatives en lien avec des vulnérabilités/incidents IT pour le système d'information

[en gras les tâches les plus impactées par les hypothèses d'évolution]

² Intrusion Prevention System

³ Intrusion Detection System

⁴ Computer Emergency Response Team

Les compétences de l'ingénieur – chargé de monitoring des incidents IT

Savoirs	Savoir-être
<p>Savoirs clés :</p> <ul style="list-style-type: none"> ○ Politique de sécurité propre à l'entreprise ○ Normes et procédures de sécurité IT ○ Normes et procédures associés aux réseaux ○ Normes, méthodes, standards, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001) ○ Lois, règles et pratiques juridiques en matières de protection des données, de la propriété intellectuelle, copyright... pour le fonctionnement des réseaux : - Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (loi Lux.) - Loi du 30 mai 2005 (relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques (loi Lux.) - Législation sur le secret professionnel, sur le secteur concerné - Règlement grand-ducal du 27 novembre 2004 (chargé de la protection des données (loi Lux.) - Rapports, circulaires, règlements fournis par les Autorités de contrôle (Commission Nationale de la Protection des Données) ○ Forensic Analysis (techniques de fonctionnement) ○ Charte d'utilisation et de sécurité des SI 	<ul style="list-style-type: none"> ○ Analyste pour savoir interpréter une situation, une documentation non conforme aux procédures de sécurité et agir en conséquence ○ Curieux afin de suivre les évolutions technologiques et réglementaires liées à l'utilisation des outils de monitoring des incidents IT Discret dans la manière de recueillir les informations et de ne pas les divulguer ○ Proactif afin de mettre à jour ses procédures d'analyse et de surveillance des incidents IT ○ Rigoureux pour s'appliquer à respecter méthodiquement la mise en œuvre des procédures liées à la gestion des incidents IT
Savoir-faire	Savoirs technologiques
<p>Savoir-faire clés :</p> <ul style="list-style-type: none"> ○ Concevoir des batteries de tests pour valider le fonctionnement des outils de monitoring ○ Configurer les outils de monitoring spécifiques au contexte/entreprise ○ Déterminer les tests à utiliser en fonction des besoins identifiés pour vérifier l'efficacité des outils de monitoring ○ Donner des inputs à la rédaction d'un cahier des charges pour les outils de monitoring, pour les besoins en monitoring ○ Elaborer des métriques en fonction des priorités que l'entreprise peut avoir définies dans sa politique sécurité ○ Elaborer son référentiel de sources d'informations (à partir de forums, newsletters, colloques...) ○ Exécuter des batteries de tests en les injectant dans le système ○ Faire évoluer des métriques identifiées ○ Formuler et exprimer correctement les recommandations et/ou risques liés aux alertes recensées ○ Identifier les éléments de preuves pour le juriste ○ Proposer des améliorations sur le fonctionnement sur Système d'Information ○ S'assurer que les flux, les échanges entre les éléments d'un réseau soient connus, dans le cadre du monitoring ○ Suivre les évolutions documentaires liées à la politique de sécurité de l'entreprise ○ Suivre les évolutions technologiques et réglementaires du domaine ○ Contrôler les accès, les flux d'informations au regard d'un document de référence tel que la politique de sécurité ○ Corréler des événements ○ Effectuer la collecte des données ○ Hiérarchiser les incidents ○ Mettre en place et configurer les sondes IDS, IPS ○ Mettre en relation des événements pour signaler l'incident à partir de plusieurs sources ○ Qualifier et détecter une alerte (faux positif) ○ S'assurer (ou l'effectuer soi-même si nécessaire) de l'isolement et du signalement des ports, PC défectueux ou non conformes ○ S'assurer (ou l'effectuer soi-même si nécessaire) de l'isolement et du signalement des zones compromises ○ S'assurer (ou l'effectuer soi-même si nécessaire) de la configuration d'un firewall, d'un antivirus ○ S'assurer (ou l'effectuer soi-même si nécessaire) du relevé et de l'interprétation des logs applicatifs, système... ○ Suivre les circuits de communication ○ Vérifier le paramétrage et la configuration des équipements et logiciels de filtrage, de détection et de refoulement mis en place 	<p>Savoirs technologiques clés :</p> <ul style="list-style-type: none"> ○ Architecture des réseaux informatiques et télécoms ○ Architecture technique du SI de l'entreprise ○ Droits d'accès aux applications et services ○ Outils d'administration de réseaux ○ Architecture fonctionnelle du SI (Système d'Information) de l'entreprise (logiciels, applications métiers) ○ Environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données, etc) ○ Architecture de systèmes d'exploitation ○ Environnement d'exploitation ○ Gestion et exploitation des SI ○ Logiciels et matériels réseaux ○ Protocoles de communication

Les compétences nouvelles pour l'ingénieur – chargé de monitoring des incidents IT

Résultats : Pour le métier de Ingénieur - Chargé de monitoring des incidents IT

Orientation de la pratique du métier	A horizon 2010, l'ingénieur - chargé de monitoring des incidents IT devra encore davantage faire preuve d'ouverture d'esprit et d'écoute vis à vis de l'environnement dans lequel il évolue. Il devra orchestrer une véritable veille pour suivre les évolutions de son activité	
Types de compétences	Éléments nouveaux exprimés par les experts	Commentaires explicatifs
Savoir	Connaissances des procédures d'escalation en lien avec la problématique de la sécurisation de l'Information mise en place dans l'organisation monitorée	
Savoir - Faire	Formuler/vulgariser les incidents IT de la manière la plus appropriée en fonction du profil de l'interlocuteur à contacter	Il s'agira de synthétiser au mieux une situation problématique pour la rendre la plus compréhensible possible et ce quelque soit le niveau fonctionnel et/ou organisationnel de l'interlocuteur
	Déterminer les personnes/compétences les plus à même de traiter un problème/un incident IT	Il aura cette responsabilité d'évaluer de la manière la plus précise/fine possible les incidents rencontrés et de faire suivre leur traitement par la personne la plus adéquate/compétente possible
	S'assurer du traitement de l'incident (de la résolution à la clôture de l'incident)	Il pourrait être demandé à l'Ingénieur Chargé de monitoring des incidents IT d'assurer un véritable suivi de la gestion de l'incident IT
Savoir - être	Elaborer et institutionaliser un dispositif de veille en lien avec la gestion des incidents IT	Il lui sera nécessaire de rester attentif à toutes évolutions (outils de monitoring, intrusions, etc) et de pouvoir le cas échéant être force de proposition pour améliorer la gestion des incidents IT au sein de son organisation
	Communicateur Force de proposition	

D. Pour le métier de Juriste en Sécurité de l'Information

Missions : Le juriste en Sécurité de l'Information, interne ou en consultance externe, conseille l'organisation dans le cadre de ses adaptations nécessaires en matière de Sécurité de l'Information (droit civil (protection des données), droit commercial (commerce électronique), droit contractuel et/ou pénal (piratage informatique)).

L'impact du scénario d'évolution sur les tâches et compétences du métier :

Les activités principales et tâches associées

<p>Prévenir l'entreprise des risques juridiques potentiels liés à des pratiques/problématiques en matière de Sécurité de l'Information</p> <ul style="list-style-type: none"> ○ Détecter les risques juridiques spécifiques au niveau de la Sécurité de l'Information pouvant affecter l'entreprise ○ Evaluer les risques juridiques liés à l'emploi et à l'utilisation TIC, lors de l'élaboration de contrats, de projets, lors de l'utilisation de logiciels, de données, lors d'archivage et de traitement des données à caractère personnel... ○ Contribuer à l'élaboration de la politique de Sécurité de l'Information, à son alignement par rapport à la politique de sécurité de l'organisation et à tout type de livrable en lien avec ces aspects 	<p>Proposer une assistance/médiation juridique à l'entreprise pour le précontentieux, le contentieux et l'arbitrage</p> <ul style="list-style-type: none"> ○ Accompagner le client/l'employeur pour des contentieux (de type civil, commercial, pénal et administratif) ○ Participer à l'évaluation des préjudices/incidents (vol de données...) ainsi qu'aux demandes de réparations des préjudices ○ Assister le client/l'employeur dans la résolution non contentieuse, gestion amiable et précontentieuse des conflits dans le cadre de missions de conciliation et de médiation
<p>Accompagner l'entreprise au niveau juridique face aux évolutions du domaine de la Sécurité de l'Information</p> <ul style="list-style-type: none"> ○ Elaborer et mettre à jour, en collaboration avec les RSSI ou équivalent, les pratiques et les procédures qui découlent des évolutions du cadre légal ou juridique du domaine de la Sécurité de l'Information ○ Proposer une assistance au RSSI, équivalent ou autres• Développer et exploiter un fonds documentaire juridique ○ Sensibiliser, informer, diffuser des informations liées à des risques juridiques potentiels ou avérés en matière de Sécurité de l'Information 	

[en gras les tâches les plus impactées par les hypothèses d'évolution]

Les compétences du juriste en sécurité de l'information

Savoirs	Savoir-être
<p>Savoirs clés :</p> <ul style="list-style-type: none"> ○ Fonctionnement des organisations (Structures organisationnelles) ○ Normes, méthodes, standards, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001) ○ Charte d'utilisation et de sécurité des SI ○ Normes et procédures de sécurité IT ○ Normes et procédures associés aux réseaux ○ Droit des Technologies de l'Information et de la Communication, de la protection des données, de la propriété intellectuelle ○ Stratégie d'entreprise ○ Environnement de l'entreprise ○ Concepts et pratiques d'investigation (Forensic) <p>A titre informatif :</p> <ul style="list-style-type: none"> - Loi modifiée du 14 août 2000 relative au commerce électronique - Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (loi Lux.) - Loi du 30 mai 2005 (relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques (loi Lux.)) - Loi sur la signature électronique - Législation sur le secret professionnel, sur le secteur concerné - Règlement grand-ducal du 27 novembre 2004 (chargés de la protection des données (loi Lux.)) - Règlements grands ducaux pour le commerce électronique - Circulaires de la Commission de Sécurité du Secteur Financier - Rapports, circulaires, règlements fournis par les Autorités de contrôle - Articles 509 -1 et suivants, du Code pénal concernant la criminalité informatique 	<p>Savoir-être clés :</p> <ul style="list-style-type: none"> ○ Aisance relationnelle afin de défendre et d'accompagner son client lors d'une affaire juridique ○ Négociateur/Médiateur dans les phases de litige ou de conciliation à l'amiable ○ Analyste pour savoir interpréter une situation non conforme par rapport à la loi et proposer des solutions ○ Synthétique pour présenter pertinemment les problèmes qu'une entreprise pourrait rencontrer si elle ne traite pas telle ou telle non-conformité, pour faire un point sur une affaire juridique avec une tierce personne ○ Intègre dans la mesure où il ne doit pas se permettre d'encourager ou de cautionner des actions qui iraient à l'encontre des règles juridiques en matière de sécurité de l'Information ○ Travailler en équipe pour échanger sur un dossier, pour savoir recueillir de l'information, pour développer un argumentaire juridique ○ Curieux face aux évolutions juridiques, réglementaires et technologiques du domaine de la Sécurité de l'Information
<p style="text-align: center;">Savoir-faire</p> <p>Savoir-faire clés :</p> <ul style="list-style-type: none"> ○ Contribuer à l'élaboration des supports de communication pour la sensibilisation des collaborateurs aux bonnes pratiques en matière de Sécurité de l'Information ○ Dialoguer - interroger- interviewer des collaborateurs, clients, ou tiers personnes ○ Identifier les non - conformités par rapport aux réglementations existantes ○ Mener des négociations ○ Rédiger / mettre en conformité des contrats, des documents à caractère juridique. ○ Transmettre les informations, documents légaux à la Commission Nationale de la Protection des Données ○ Analyser les pratiques de l'organisation en matière d'archivage, de droit d'accès des documents papiers/électroniques ○ Analyser et interpréter des textes législatifs ou réglementaires nationaux, la réglementation communautaire et la jurisprudence ○ Préparer un argumentaire juridique ○ Suivre les évolutions juridiques, réglementaires et technologiques liées à la Sécurité de l'Information ○ 	<p style="text-align: center;">Savoirs technologiques (Maîtrise des risques juridiques liés à la mise en œuvre de ces différents savoirs)</p> <ul style="list-style-type: none"> ○ Connaissances des différentes architectures métier, fonctionnelle, applicative et technique ○ Connaissances de l'environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données...) ○ Connaissances des différents logiciels et matériels réseaux ○ Connaissances des outils d'administration de réseaux ○ Connaissances de la gestion des droits/ Identity & Privilege Management

Les Compétences nouvelles pour le juriste en sécurité de l'information

Orientation de la pratique du métier	<p>Les compétences relationnelles du profil professionnel actuel de Juriste en Sécurité de l'Information (Négociateur/médiateur, Analyste, Synthétique, Intègre, Travail d'équipe, Aisance relationnelle, Curieux) s'affirmeront à terme dans la pratique du métier</p> <p>L'une d'entre elles est primordiale, il s'agit de la curiosité vers le domaine de l'IT. Il devra être capable de comprendre les flux de données, d'informations au sein de l'organisation, la manière dont l'infrastructure de l'entreprise et son activité fonctionne. A ce titre, il devra s'attacher à développer une certaine culture informatique de base. Il sera alors en mesure de poser les bonnes questions pour identifier, anticiper des problèmes à venir au sein de l'organisation pour laquelle il travaille.</p> <p>Au niveau du positionnement de ce métier au sein de l'organisation, il est pressenti que ce dernier se situera à un niveau transverse, d'un point de vue organisationnel. Il assurera les relations entre des services IT et Juridique. Il devra rester en contact avec chacun d'entre eux, notamment pour suivre les changements de toutes natures que chacun de ces départements peuvent subir ou impulser.</p> <p>La reconnaissance de son action au sein d'une organisation dépendra de son positionnement avec le métier de RSSI et de la densité de leur relation.</p> <p>Si le Juriste en Sécurité de l'Information est considéré comme le véritable bras armé juridique du RSSI, alors le premier sera en mesure d'avoir toute la légitimité nécessaire à son action au sein d'une organisation</p>	
Types de compétences	Éléments nouveaux exprimés par les experts	Commentaires explicatifs
Savoir	<p>Connaissance accrue du core business de l'organisation dans lequel il évolue ainsi que de son contexte organisationnel, de sa culture, des projets et des solutions mises en œuvre</p> <p>Connaissances des modalités d'intervention des services de police, de justice, ainsi que des organismes de contrôle et d'accréditation, etc au sein des entreprises</p>	<p>Il pourra ainsi identifier au mieux les problématique liées à la Sécurisation des systèmes d'Information et aux risques juridiques qui y sont liés. La question de l'identification de ces risques est primordial car elle facilitera la mise en oeuvre de mesures et moyens pour y faire face ou les couvrir.</p> <p>Il s'agira en effet pour ce professionnel d'appréhender au mieux les modes opératoires de la police Luxembourgeoise afin de savoir comment doit répondre une organisation par rapport aux modalités d'intervention de la police.</p>
Savoir - Faire	<p>Orchestrer une mise à jour des pratiques de l'entreprise suite au renouvellement de l'activité de l'entreprise et des changements que cela implique</p> <p>Identifier les compétences extérieures nécessaires pour une situation qui paraît trop complexe</p> <p>S'inscrire dans une logique de négociation "gagnant-gagnant" lorsque cela s'avère utile dans les phases de gestion post incidents et/ou précontentieux</p> <p>Assister l'entreprise dans la mise en place de démarche de certification ou de conformité (certification ISO 27001 notamment) d'un point de vue juridique en terme de prévention</p> <p>Mettre en place des actions de sensibilisation en lien avec ses problématiques pour permettre à l'organisation de se prémunir des phénomènes de résistance au changement de la part des salariés</p> <p>Vulgariser et communiquer de l'information juridiques auprès de différents interlocuteurs</p>	<p>Il ne s'agit pas dans ce cas présent d'instituer une veille structurée d'un point de vue juridique. L'évolution juridique ne semble pas assez significative pour que le Juriste en Sécurité de l'Information soit obligé de mettre en oeuvre des pratiques de veille structurées. Par contre, il devra en être autrement pour le suivi des évolutions de l'entreprise, de ses produits et/ou services. Il paraît primordial au regard des experts présents de suivre le changement que génère par exemple l'apparition d'une nouvelle offre de services/produits au sein même d'une organisation. Des nouveaux risques juridiques sont à appréhender au niveau des problématiques liées à la Sécurisation de l'Information</p> <p>Il est fait mention du cas où le Juriste en Sécurité de l'Information exerce son activité au sein même d'une organisation. Il se peut dans cette hypothèse que le professionnel doive recourir à un cabinet juridique spécialisé en externe. Cela paraît particulièrement judicieux lorsque des situations d'urgence et de grandes ampleurs sont constatées ou qu'un apport d'expertise externe ait identifié.</p> <p>Il s'agit de s'interroger sur la nécessité de rentrer dans une logique de confrontation ou non</p> <p>Le juriste pourra alors définir plus clairement pour l'organisation le périmètre et la signification exacte des résultats d'une telle démarche.</p> <p>Cela permettra ainsi d'améliorer le niveau de maturité des pratiques professionnelles manipulant de l'information.</p> <p>La vulgarisation des termes techniques juridiques auprès de différents interlocuteurs apparaît importante dans la mesure où ces derniers ne sont pas forcément familiarisés au langage professionnel d'un juriste en Sécurité de l'Information</p> <p>Qui plus est, la vulgarisation des termes techniques juridiques doit être mis en oeuvre dans des échanges d'ordre vertical ou horizontal. Le but est d'intégrer le juridique dans la culture de base de l'entreprise du salarié.</p>
Savoir - être	<p>Réagir "positivement" à une situation d'urgence tout en proposant une assistance juridique en Sécurité de l'Information</p>	<p>Par cette expression, les experts ont voulu insister sur la nécessité qu'un Juriste en Sécurité de l'Information aura de savoir rebondir face à des situations critiques et/ou urgentes</p>

Références

- Barbolosi. P., Hua D. (2007) « Quelle évolution pour l'environnement du Manager Logistique au Luxembourg ? », Centre de Recherche Public Henri Tudor, Luxembourg.
- Durand A., (2004), "Anticiper l'évolution des compétences en Technologie de l'Information et de la Communication : une application au métier d'entrepreneur de construction", Centre de Recherche Public Henri Tudor, Luxembourg.
- Durand A., (2005), "Module d'assistance au lancement des Comités d'Accompagnement de Plate-forme d'innovation du CITI", Centre de Recherche Public Henri Tudor, Luxembourg.
- Fericelli A.-M, (2001), "Théorie de la décision", Dictionnaire des Sciences Economiques, PUF.
- Godet M., (2001), "Manuel de prospective stratégique". Dunod.
- Meunier B, Hua D, (2007) « Anticipation des compétences du métier de Manager Logistique à Horizon 2010 », Centre de Recherche Public Henri Tudor, Luxembourg.