

# Anticipation des compétences du métier de Consultant en Sécurité de l'Information à horizon 2010

## Résumé

Le présent document expose le résultat d'une réflexion structurée, menée par **12 professionnels du domaine de la Sécurité de l'Information** qui se sont attachés à **analyser l'évolution spécifique du métier de Consultant en Sécurité de l'Information au Grand-Duché du Luxembourg d'ici 2010.**

En fonction de l'horizon ciblé, ces professionnels ont construit ensemble un scénario d'évolution pour le domaine de la Sécurité de l'Information. Ils ont ensuite mesuré son impact sur les compétences existantes du métier. **Une vingtaine de compétences a été identifiée comme clés** pour les trois à cinq ans à venir. Les experts ont complété leur réflexion par un travail de projection sur les éléments nouveaux (compétences, responsabilités, prérogatives) que la vision du métier traitée devra intégrer à moyen terme. A ce titre, **7 compétences nouvelles ont été recensées.**

**Mots-clés :** compétences, formation, anticipation, sécurité de l'information, Consultant

CITI

Centre de Recherche Public Henri Tudor  
29, Avenue John F.Kennedy  
L-1855 Luxembourg - Kirchberg  
Tél.: +352 42 59 91 - 1  
Fax: +352 42 48 99 - 777

Rédigé par Bertrand Meunier<sup>1</sup>, Duan Hua<sup>2</sup>, Alex Durand<sup>3</sup>, Frédéric Girard<sup>4</sup>

<sup>1</sup>bertrand.meunier@tudor.lu - Chef de projet R&D

<sup>2</sup>duan.hua@tudor.lu - Expert méthode

<sup>3</sup>alex.durand@tudor.lu - Coordinateur Scientifique

<sup>4</sup>frederic.girard@tudor.lu - Reviewer

[www.citi.tudor.lu](http://www.citi.tudor.lu)

## Remerciements

L'équipe du projet Abilitic<sup>1</sup> adresse ses remerciements à :

- Monsieur BOUAOUD Malike (IT WORKS)
- Monsieur DANN Philippe (UBIZEN)
- Monsieur DE PRIL Yves (CONOSTIX)
- Monsieur FELTUS Christophe (CRP Henri TUDOR)
- Monsieur GIRARD Frédéric (CRP Henri TUDOR)
- Monsieur KAYSER Jean Yves (Chambre des métiers)
- Monsieur MARIS Koen (CONOSTIX)
- Monsieur MAUNY Cédric (TELINDUS)
- Monsieur MELLINGER Laurent (Secaron)
- Monsieur MOUREAU Michel (ECONOCOM)
- Madame PELTIER Noelle (CRP Henri TUDOR)
- Monsieur POGGI Sébastien (CRP Henri TUDOR)

Pour leur contribution, et leur participation active à cette réflexion sur le thème de l'anticipation des compétences du métier de Consultant en Sécurité de l'Information.

---

<sup>1</sup> Le projet Abilitic est un projet Interreg3A visant à anticiper à moyen terme l'évolution des compétences pour 8 métiers à un niveau inter – régional. De plus amples informations sur le site [www.abilitic.eu](http://www.abilitic.eu)

## Table des matières

Introduction.....	4
I. Méthodologie.....	5
II. Phase n°1 : Le profil professionnel .....	6
1. La structure .....	6
2. Les Missions .....	6
3. Activités et tâches associés du métier Consultant en Sécurité de l'Information.....	8
4. Les Compétences principales du métier .....	9
III. Phase n°2 : Le profil d'évolution du métier Consultant en Sécurité de l'Information .....	10
1. Le Scénario d'évolution .....	10
2. Le plan d'actions .....	11
IV. Phase n°3 : Les tendances à venir du profil de formation .....	16
1. Les activités et tâches du métier impactées par le changement .....	16
2. Les compétences clés du Consultant en Sécurité de l'Information.....	19
3. Les compétences nouvelles pour le Consultant en Sécurité de l'Information .....	24
4. Canevas d'investigation à l'attention des organismes de formation.....	26
Conclusion .....	27
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. Celle-ci a pour objectif d'identifier aujourd'hui les compétences dont des professionnels auront besoin demain, à moyen terme (3-5 ans), dans l'exercice de leur métier. Les résultats d'un tel exercice doivent permettre à l'offre de formation existante de s'interroger au plus tôt sur les programmes de formation. Cela doit représenter un outil d'aide à la décision facilitant et appuyant la définition le cas échéant de nouveaux programmes de formation. Ces derniers seront ainsi en mesure de répondre au plus près des préoccupations de la demande émanant des professionnels d'un métier.

Le présent document a pour objectif de montrer qu'il est possible d'envisager le déploiement d'un tel exercice pour le métier de Consultant en Sécurité de l'Information au Grand-Duché du Luxembourg.

Les professionnels de la Sécurité de l'Information qui ont mené cette réflexion, ont commencé par identifier les changements essentiels auxquels le Luxembourg sera confronté d'ici 2010 pour le domaine de la Sécurité de l'Information au Luxembourg. Ces changements ont déjà fait l'objet d'un rapport documenté<sup>2</sup>. Il s'agit des mutations que devrait connaître l'environnement du métier étudié à horizon 2010. L'ensemble de ces mutations compose le scénario d'évolution.

Ensuite, ces professionnels ont mesuré l'impact du changement sur les compétences actuelles du métier de Consultant en Sécurité de l'Information. Ils ont également défini les compétences nouvelles qu'il faudra acquérir pour se préparer au changement.

L'étude se décompose donc en quatre parties. Une première partie est consacrée à un rappel méthodologique des différentes étapes constitutives de la démarche d'anticipation des compétences. Une seconde partie porte sur la présentation de la vision du métier de Consultant en Sécurité de l'Information. Une troisième partie s'intéresse à la présentation du scénario d'évolution du métier étudié. Enfin, la quatrième et dernière partie se focalise quant à elle sur les compétences actuelles et nouvelles qu'un Consultant en Sécurité de l'Information devra maîtriser demain dans l'exercice de sa fonction.

---

<sup>2</sup> Hua D, Meunier B, Girard F, Durand A (2007) « La Sécurité de l'Information au Grand Duché du Luxembourg en 2010 ? », Centre de Recherche Public Henri Tudor, Luxembourg.

## I. Méthodologie

La démarche prospective proposée a pour premier objectif d'anticiper les évolutions possibles de l'environnement du métier de Consultant en Sécurité de l'Information au Luxembourg à 3-5 ans, et d'identifier des actions permettant soit de se préparer vis-à-vis du futur probable, soit de pro-agir pour la réalisation d'un futur souhaité. Son second objectif est de détecter les futurs besoins en compétences du métier sélectionné d'ici 2010. En réponse à ces besoins les organismes de formation pourront être en mesure de concevoir et de proposer une offre de formation adaptée aux besoins exprimés du marché.

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 entretiens avec des « experts » métier ayant une vision de l'exercice du métier.
- Entretiens individuels avec différents responsables dans le domaine de la Sécurité de l'Information.

### **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, responsables dans le 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 formations existantes correspondantes ou à créer.

**Démarche** :

Une séance de groupe de travail réunissant le même type d'acteurs.

Les résultats obtenus en matière d'anticipation des compétences du métier Consultant en Sécurité de l'Information seront présentés en fonction des trois étapes de la démarche.

## II. Phase n°1 : Le profil professionnel

### 1. La structure

Le profil professionnel décrit le travail que les professionnels accomplissent dans le cadre de leur métier ou de leur profession. Le métier de Consultant en Sécurité de l'Information est présenté 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 **activité**. 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 une subdivision de l'activité ; 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.

Le profil professionnel du métier de Consultant en Sécurité de l'Information étant conséquent, il est disponible sur le site [www.abilitic.eu](http://www.abilitic.eu). Afin de prendre connaissance toutefois du document dans sa globalité, une version synthétique a été conçue. Celle-ci se décompose en plusieurs sections. Premièrement, une description des missions attendues par le métier a été formalisée. Deuxièmement, cette version expose l'ensemble des activités et des tâches associées au métier sélectionné. Troisièmement, l'ensemble des compétences principales du métier est regroupé au sein d'un tableau qui est composé de quatre sous-ensembles représentant les principaux savoirs, savoir-être, savoir-faire et savoirs technologiques recensés pour l'exercice de la fonction de Consultant en Sécurité de l'Information.

### 2. Les Missions

Il s'agit de la vision du métier à partir de laquelle les parties prenantes du projet, le CRP Henri Tudor ainsi que les partenaires experts dans le domaine étudié ont souhaité travailler. Ainsi le **rôle de Consultant en Sécurité de l'information a été défini de la manière suivante. Il a ainsi pour rôle 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.**

Le choix a été fait dans l'étude du devenir de ce métier de l'appréhender exclusivement comme un prestataire, un intervenant externe à une entreprise. Il n'a pas été envisagé dans ce travail de formalisation de l'appréhender comme un conseiller interne à l'organisation.

Qui est plus, le champ de ces prérogatives a été défini de telle sorte à ce que le Consultant en Sécurité de l'Information soit en mesure d'intervenir en tant qu'assistant à la fois à la Maîtrise d'Ouvrage et au Maître d'œuvre. Ces activités ont été formalisées, de telle sorte à ce que ses actions en tant que Consultant en Sécurité de l'Information puissent avoir un impact, en fonction de la mission confiée, sur les niveaux de décision opérationnels, tactiques (intermédiaires) et stratégiques de l'entreprise dans laquelle il est amené à intervenir.

L'ensemble de ses missions est présenté à travers les 5 activités détaillées ci après :

- Prendre en charge les enjeux et les spécificités du client
- Collaborer au développement de la prestation en assistant la Maîtrise d'Ouvrage (MOA) et la maîtrise d'œuvre (MOE).
- Accompagner l'aide au changement par des actions de communication et de formation

Les deux premières activités correspondent à la fonction même d'un Consultant en Sécurité de l'Information. C'est dans le cadre des actions qui y sont associées que le Consultant en Sécurité de l'Information déploiera son savoir-faire critique au sein d'une organisation. La plus value personnelle de son travail se situe dans la réalisation des tâches liées à ces deux activités.

Par ailleurs, une activité d'accompagnement au changement a été intégrée de manière distincte à ce métier. Les experts qui ont participé à la définition du métier, ont souhaité mettre en avant l'intérêt de faire valoir ce type d'activité. Il est important en effet pour les experts présents que les Consultants en Sécurité de l'Information, dans l'exécution de leurs missions, la présentation de leurs travaux, puissent faire mieux comprendre et accepter les solutions proposées par rapport aux problèmes rencontrés.

Le contenu de ces activités est détaillé dans le premier tableau ci après. Il s'agit des tâches qui y sont associés. Un second tableau s'attache quant à lui à indiquer l'ensemble des compétences principales qui ont été identifiées pour le métier de Consultant en Sécurité de l'Information aujourd'hui.

Au niveau des savoirs technologiques, il ne s'agit pas pour le Consultant en Sécurité de l'Information d'être expert dans l'utilisation et l'exploitation des compétences identifiées. Il lui faut autant que possible comprendre les fonctionnalités génériques des outils qui peuvent répondre à tout ou partie des problématiques identifiées chez un client.

### 3. Activités et tâches associés du métier Consultant en Sécurité de l'Information

<p><b>Activité 1 : Prendre en charge les enjeux et les spécificités du client</b></p> <ul style="list-style-type: none"> <li>• Prendre connaissance de l'existant</li> <li>• Comprendre les spécificités du client</li> <li>• Comprendre le fonctionnement interne de l'entreprise</li> <li>• Analyser les besoins</li> <li>• Traduire les spécificités fonctionnelles et non fonctionnelles en plans d'actions, en politique de sécurité, etc</li> <li>• Assurer un pilotage stratégique</li> </ul>	<p><b>Activité 2 : Collaborer au développement de la prestation en assistant à la Maîtrise d'Ouvrage (MOA) et la Maîtrise d'œuvre (MOE)</b></p> <ul style="list-style-type: none"> <li>• Formaliser l'analyse de l'existant</li> <li>• Formaliser les conclusions de l'analyse</li> <li>• Assurer l'adéquation entre les recommandations proposées et la mise en œuvre des solutions</li> <li>• Participer à l'élaboration d'un cahier des charges</li> <li>• Etudier les intégrateurs, les distributeurs et les solutions du marché</li> <li>• Evaluer les solutions proposées</li> <li>• Participer à l'élaboration de l'expression des besoins</li> <li>• Négocier si besoin à la contractualisation de la relation MOA/MOE</li> <li>• Valider les livrables (recettes)</li> </ul>
<p><b>Activité 3 : Accompagner l'aide au changement par des actions de communication et de formation</b></p> <ul style="list-style-type: none"> <li>• Encadrer le client dans son apprentissage des enjeux liés à la Sécurité de l'Information</li> <li>• Définir et appliquer le schéma de communication en lien avec la ou les solutions proposées</li> <li>• Personnaliser son langage en fonction des collaborateurs rencontrés</li> <li>• Se former aux évolutions du domaine de la Sécurité de l'Information et aux pratiques et stratégies des entreprises.</li> </ul>	

## 4. Les Compétences principales du métier

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

### III. Phase n°2 : Le profil d'évolution du métier Consultant en Sécurité de l'Information

#### 1. Le Scénario d'évolution

Le scénario d'évolution est construit à partir des déterminants de l'évolution du domaine du métier étudié au Luxembourg d'ici 2010. De nature réglementaire, normative, technologique, économique, sociale, culturelle et organisationnelle, relevant d'un environnement national et international, ces déterminants ont été identifiés comme ceux qui expliqueront demain l'évolution du domaine du métier sélectionné.

Le tableau ci-dessous présente le scénario d'évolution. Il expose à la fois les différents facteurs d'évolution essentiels ainsi que les différentes hypothèses d'évolution qui ont été retenues pour l'évolution de l'environnement du métier de Consultant en Sécurité de l'Information. Pour connaître ses modalités d'élaboration, un rapport<sup>3</sup> documenté sur l'ensemble des étapes ayant permis sa construction est disponible sur le site : [www.abilitic.eu](http://www.abilitic.eu).

N°	Intitulés des facteurs d'évolution essentiels	Hypothèses d'évolution retenues
1	<i>Absence d'une entité d'assistance (Computer Emergency Response Team : CERT)</i>	En 2010, émergence d'une entité d'assistance (CERT) au Grand Duché du Luxembourg
2	<i>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)
3	<i>Evolution 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
4	<i>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
5	<i>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)
6	<i>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
7	<i>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)
8	<i>Les Systèmes d'Information et de la Communication, infrastructures critiques au même titre que l'eau et l'électricité</i>	En 2010, la criticité des Systèmes d'Information et de Communication se fera de plus en plus importantes au même titre que des ressources primaires (eau, électricité) : forte dépendance de la part des entreprises/organisations vis à vis des SIC
9	<i>Evolution 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 fiabilités des systèmes, redondance des moyens informatiques)
10	<i>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

<sup>3</sup> Hua D, Meunier B, Girard F, Durand A (2007) « La Sécurité de l'Information au Grand Duché du Luxembourg en 2010 ? », Centre de Recherche Public Henri Tudor, Luxembourg.

## 2. Le plan d'actions

Le scénario d'évolution identifié, il convient maintenant de réfléchir aux moyens à mettre en œuvre pour le rendre effectif. Pour chaque évolution, le groupe de travail propose une série d'actions qui permettront de se préparer et d'atteindre les évolutions ainsi identifiées. Les actions considérées comme prioritaires par les experts sont **mises en évidence**.

### **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 luxembourgeoises. Il a même été suggéré d'acquérir 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 du département Marketing au sein des entreprises qui vendent des technologies. Ces derniers sont en effet sensibles aux conséquences commerciales suite à des accidents/incidents 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'autre 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 le référentiel de compétences est présenté ci après. Cela permet d'identifier les compétences clés du métier de Consultant en Sécurité de l'Information à horizon 2010 et d'envisager quels sont les éléments nouveaux à intégrer en terme de compétences pour ce métier.

## IV. Phase n°3 : Les tendances à venir du profil de formation

Cette phase n°3 se décompose en plusieurs parties. Les trois premières parties décrivent sur base des activités et des tâches du métier les plus impactées par le scénario d'évolution, les compétences actuelles et nouvelles qu'un professionnel devra veiller à maîtriser demain dans l'exercice de son métier. La dernière partie s'évertue présenter à canevas d'investigation que les organismes de formation devraient investir pour élaborer un programme répondant aux défis à venir du métier de Consultant en Sécurité de l'Information.

### 1. Les activités et tâches du métier impactées par le changement

Il s'agit ici de mesurer l'impact des changements décrits par le scénario d'évolution sur le profil professionnel du métier de Consultant en Sécurité de l'Information. Le but est de sélectionner les tâches les plus impactées par le changement. A l'issue de la mesure d'impact **neuf tâches ont été sélectionnées et considérées comme susceptibles d'évoluer fortement face aux changements pressentis pour le domaine de la Sécurité de l'Information.**

Au regard de la mesure d'impact, il apparaît que **toutes les activités du métier étudié ont été impactées par le scénario d'évolution du domaine de la Sécurité de l'Information.** En d'autres termes, aucune activité du métier ne devrait être « épargnée » par les évolutions pressenties pour le domaine étudié. Chaque activité a en effet au minimum 2 tâches impactées par le scénario d'évolution.

Les activités du métier ne seraient toutefois pas impactées à même hauteur. En effet, sur les dix hypothèses composant le scénario d'évolution, sept ont été identifiées comme étant susceptibles de faire évoluer les quatre tâches retenues de l'activité 1 « *Prendre en charge des enjeux et spécificités du client* », six pour les trois tâches de l'activité 3 « *Accompagner l'aide au changement par des actions de communication et de formation* » et trois pour les deux tâches de l'activité 2 « *Collaborer au développement de la prestation en assistant la MOA et la MOE* ». La pratique de l'activité 1 semble donc prépondérante dans l'évolution du métier de Consultant selon les experts qui ont participé à l'évaluation. Il appartiendra donc aux acteurs du monde pédagogique, de veiller à l'intégration de cette tendance dans le contenu des formations qui pourrait être proposé à des consultants expérimentés ou non.

Par ailleurs, il est à noter qu'une hypothèse d'évolution sur les dix impacterait la pratique de trois tâches appartenant chacune à une activité différente. C'est le cas pour l'évolution liée à la **mise en place obligatoire d'un niveau de sécurité minimum, dictée par les autorités compétentes (administratives et/ou réglementaires) pour les entreprises de certains secteurs régulés comme le secteur financier.** Elle influencerait les tâches :

- 1.5 « *Traduire les spécificités fonctionnelles et non fonctionnelles en plans d'actions, en politique de sécurité, etc* »
- 2.3 « *Assurer l'adéquation entre les recommandations proposées et la mise en œuvre de solutions* »
- 3.4 « *Se former aux évolutions du domaine de la Sécurité de l'Information et aux pratiques et stratégies des entreprises* »

Il est donc nécessaire de rester vigilant à l'apparition ou non de cette évolution pour la pratique globale du métier de Consultant. La compréhension et l'interprétation de ce niveau de sécurité minimum influenceront indéniablement les propositions d'expertise qu'un Consultant pourra être amené à apporter, à horizon 2010.

A un degré moindre, d'autres évolutions impacteront plusieurs tâches au sein de deux activités respectives. Il s'agit des évolutions liées à :

- **La convergence de la qualité et de la sécurité grâce à l'intégration de la sécurité dans les normes qualité (ISO)** pour les tâches 1.5 « Traduire les spécificités fonctionnelles et non fonctionnelles en plans d'actions, en politique de sécurité, etc » - 1.6 « Assurer un pilotage stratégique » et 3.4 « Se former aux évolutions du domaine de la Sécurité de l'Information et aux pratiques et stratégies des entreprises »
- **La criticité des Systèmes d'Information et de Communication qui sera de plus en plus importantes au même titre que des ressources primaires (eau, électricité)** pour les tâches « 1.4 Analyser les besoins » - « 1.6 Assurer un pilotage stratégique » et « 3.1 Encadrer le client dans son apprentissage des enjeux liés à la Sécurité de l'Information »

Il est important de signaler également que certaines hypothèses ont une influence spécifique sur une seule activité du métier. C'est le cas des évolutions suivantes qui auront selon les experts, chacune une emprise sur la pratique de deux tâches d'une même activité :

- Pour l'évolution liée à l'impact de la **réduction d'éventuelles catastrophes numériques grâce à une systématisation/amélioration de l'analyse des risques et de la gestion des crises**, l'activité 1 avec les tâches 1.5 « Traduire les spécificités fonctionnelles et non fonctionnelles en plans d'actions, en politique de sécurité » et « 1.6 assurer un pilotage stratégique »,
- Pour l'évolution liée à **l'auto régulation du marché et la mise en place de codes de bonnes conduites**, etc, l'activité 2 avec les tâches 2.5 « Etudier les intégrateurs, les distributeurs et les solutions du marché » et 2.6 « Evaluer les solutions proposées. »

Cette caractéristique de chacune des activités citées doit permettre d'appréhender avec davantage de visibilité les orientations à donner à la préparation des tâches sélectionnées. Les hypothèses d'évolution mentionnées peuvent avoir, qui plus est, une influence plus large sur les autres tâches du métier liées à ces activités.

Pour finir cet exposé détaillant le degré d'influence des hypothèses d'évolutions sur les activités & tâches du métier de Consultant, il est intéressant de préciser que certaines n'impacteront qu'une seule et unique tâche :

- **l'intégration du Risk Management plus homogène grâce à sa promotion et à la prise de conscience des entreprises** pour la tâche 1.2 « comprendre les spécificités du client »
- **l'intensification du travail de sensibilisation des pouvoirs publics aux enjeux liés à la Sécurité de l'Information** pour la tâche 3.1 « Encadrer le client dans son apprentissage des enjeux liés à la Sécurité de l'Information »
- **l'émergence d'un CERT au Grand-duché du Luxembourg** pour la tâche 3.4 « Se former aux évolutions du domaine de la Sécurité de l'Information et aux pratiques et stratégies des entreprises »

Le descriptif présenté précédemment a permis de comprendre le degré d'impact des futurs enjeux auxquels le Consultant en Sécurité de l'Information devra faire face. Cela doit permettre de comprendre vers quel type d'évolution vont tendre les tâches sélectionnées.

Pour autant, il apparaît utile en complément, pour affiner la compréhension du devenir du métier, de faire un focus sur certaines tâches même du métier.

Ainsi, Il est important de signaler que 3 tâches sur les neuf ont été impactées respectivement par une seule et unique évolution.

Il s'agit des tâches :

- 1.2 « *comprendre les spécificités du métier* » pour l'hypothèse d'évolution liée à une intégration du risk management plus homogène grâce à une promotion et une prise de conscience des entreprises,
- 2.3 « *Assurer l'adéquation entre les recommandations proposées et la mise en œuvre des solutions* » pour l'évolution liée à l'obligation de mettre en place un niveau de sécurité minimum que les autorités compétentes (administratives et/ou réglementaires) établiront d'ici 2010.
- 2.5 « *Etudier les intégrateurs, les distributeurs et les solutions du marché* » par rapport à l'auto régulation espérée du marché pour la mise en place par les ISP de codes de bonnes conduites en matière de Sécurité de l'Information.

Cette caractéristique doit permettre d'appréhender au mieux dans quelles perspectives la mise en œuvre de ces tâches s'opèrera, à la différence d'autres tâches qui sont impactées par de multiples hypothèses d'évolution.

Les tâches suivantes seront en effet fortement impactées selon les experts par le devenir pressenti pour le domaine de la Sécurité de l'Information. Trois hypothèses d'évolution au minimum sont en mesure d'avoir une influence sur l'évolution de leurs pratiques. Il s'agit des tâches suivantes :

- Pour l'activité 1, la tâche 1.5 « Traduire les spécificités fonctionnelles et non fonctionnelles en plans d'actions, en politique de sécurité, etc », ainsi que la tâche 1.6 « Assurer un pilotage stratégique »
- Pour l'activité 3, la tâche 3.4 « Se former aux évolutions du domaine de la Sécurité de l'Information et aux pratiques et stratégies des entreprises. »

Dans un futur proche, un consultant devra donc se montrer vigilant dans la mise en œuvre de ces tâches, de par les besoins en terme de compétence que chacune des hypothèses d'évolution, vont engendrer.

**Les hypothèses d'évolution les plus influentes, ayant été mises en lumière, les tâches les plus significatives également, il apparaît possible maintenant de préciser les compétences indispensables à la mise en œuvre des tâches sélectionnées.**

## 2. Les compétences clés du Consultant en Sécurité de l'Information

Les compétences essentielles à la réalisation des tâches les plus impactées par le changement constituent les **compétences clés**. Le tableau ci-dessous reprend le profil professionnel dans son intégralité et indique les tâches les plus impactées avec l'ensemble des compétences clés associées. Les compétences clés sont classées en fonction du nombre de points qu'elles ont obtenus lors de l'évaluation des experts. Plus une compétence a de points, plus sa position est haute dans le classement des compétences clés pour une tâche.

### Pour l'activité 1 : Prendre en charge des enjeux et spécificités du client

Scénario d'évolution	Tâches	Compétences Clés
En 2010, l'intégration du Risk Management sera plus homogène grâce à sa promotion et à la prise de conscience des entreprises	1.2 Comprendre les spécificités du client	<ul style="list-style-type: none"> <li>• Aïssance relationnelle</li> <li>• Fonctionnement des organisations</li> <li>• Réaliser un diagnostic des besoins et analyser l'existant</li> <li>• Environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données...)</li> <li>• Disponible</li> <li>• Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001)</li> <li>• Identifier la taille, la nature et la complexité de l'organisation analysée</li> </ul>
<p>En 2010, il y aura une prise en compte de la sécurité dès la phase de conception dans les technologies</p> <p>En 2010, la criticité des Systèmes d'Information et de Communication se fera de plus en plus importantes au même titre que des ressources primaires (eau, électricité) : forte dépendance de la part des entreprises/organisations vis à vis des SIC</p>	1.4 Analyser les besoins	<ul style="list-style-type: none"> <li>• Identifier la taille, la nature et la complexité de l'organisation analysée</li> <li>• Processus business</li> <li>• Méthodes de gestion et analyse des risques (Ebios, Mehari, Marion, Melisa, Cramm, Octave)</li> <li>• Normes et procédures de sécurité IT</li> </ul>
<p>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 fiabilités des systèmes, redondance des moyens informatiques)</p> <p>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)</p> <p>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)</p> <p>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</p>	1.5 Traduire les spécificités fonctionnelles et non fonctionnelles en plans d'actions, en politique de sécurité, etc	<ul style="list-style-type: none"> <li>• Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001)</li> <li>• Normes professionnelles d'audit (IA, ISACA, etc)</li> <li>• Règles et pratiques juridiques en matière de protection des données, protection de la propriété intellectuelle, copyright</li> <li>• Rigoureux</li> <li>• Intégration de nouvelles technologies au SI</li> </ul>

<p>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)</p>	<p>1.6 Assurer un pilotage stratégique</p>	<ul style="list-style-type: none"> <li>• Gestion et conduite de projet</li> <li>• Animer et préparer des réunions</li> <li>• Stratégie d'entreprise</li> <li>• Mettre en conformité l'organisation</li> <li>• Réaliser l'évaluation d'une situation, d'avancement</li> <li>• Savoir s'adapter à différents types d'interlocuteurs</li> <li>• Disponible – à l'écoute</li> </ul>
<p>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 fiabilités des systèmes, redondance des moyens informatiques)</p>		
<p>En 2010, la criticité des Systèmes d'Information et de Communication se fera de plus en plus importantes au même titre que des ressources primaires (eau, électricité) : forte dépendance de la part des entreprises/organisations vis à vis des SIC</p>		

**Pour l'activité 2 :** Collaborer au développement de la prestation en assistant la Maîtrise d'Ouvrage et la Maîtrise d'œuvre

Scénario d'évolution	Tâches	Compétences Clés
<p>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)</p>	<p>2.3 Assurer l'adéquation entre les recommandations proposées et la mise en œuvre des solutions</p>	<ul style="list-style-type: none"> <li>• Gestion du changement</li> <li>• Intégration de nouvelles technologies au SI</li> <li>• Mettre en conformité l'organisation</li> </ul>
<p>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</p>	<p>2.5 Etudier les intégrateurs, les distributeurs et les solutions du marché</p>	<ul style="list-style-type: none"> <li>• Intégration de nouvelles technologies au SI</li> <li>• Architecture des réseaux informatiques et télécom</li> <li>• Effectuer une veille concurrentielle</li> <li>• Veille technologique</li> <li>• Réaliser des études d'impact, des études de marché (fournisseurs)</li> </ul>
<p>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</p>	<p>2.6 Evaluer les solutions proposées</p>	<ul style="list-style-type: none"> <li>• Connaître l'environnement technique et comprendre les solutions proposées à travers le langage commercial</li> <li>• Valider une solution informatique</li> <li>• Intégration de nouvelles technologies au SI</li> </ul>
<p>En 2010, il y aura une prise en compte de la sécurité dès la phase de conception dans les technologies</p>		<ul style="list-style-type: none"> <li>• Rigoureux – méthodique</li> <li>• Environnement de l'entreprise</li> </ul>

**Pour l'activité 3 :** Accompagner l'aide au changement par des actions de communication et de formation

Scénario d'évolution	Tâches	Compétences Clés
<p>En 2010, les pouvoirs publics et les associations intensifieront la sensibilisation à la Sécurité de l'Information (multiplication des cibles)</p> <p>En 2010, la criticité des Systèmes d'Information et de Communication se fera de plus en plus importantes au même titre que des ressources primaires (eau, électricité) : forte dépendance de la part des entreprises/organisations vis à vis des SIC</p>	<p>3.1 Encadrer le client dans son apprentissage des enjeux liés à la Sécurité de l'Information</p>	<ul style="list-style-type: none"> <li>• Identifier les besoins en connaissances du client</li> <li>• Aisance relationnelle</li> <li>• Gestion du changement</li> <li>• S'adapter à différents interlocuteurs</li> </ul>

En 2010, émergence d'une entité d'assistance (CERT) au Grand-duché du Luxembourg	3.4 Se former aux évolutions du domaine de la Sécurité de l'Information et aux pratiques et stratégies des entreprises	<ul style="list-style-type: none"> <li>• Veille technologique</li> <li>• Ouvert d'esprit</li> </ul>
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		
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)		
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)		

⇒ Retour sur les compétences clés à mettre en avant dans la pratique du métier

Tout d'abord, il est intéressant de relever que l'étendue des compétences clés attendues pour un Consultant en Sécurité de l'Information apparaît conséquente, au regard des évaluations des experts. Plus d'une vingtaine de compétences clés ont été identifiées. Cela appuie l'idée selon laquelle ce métier est exigeant pour répondre au mieux aux attentes des clients.

Au niveau des résultats même, certaines compétences clés le sont, pour plusieurs tâches d'une même activité ou d'activités différentes. Six compétences se caractérisent ainsi par cette spécificité.

Dans le tableau ci après, chaque compétence clé dite redondante est présentée et reliée aux tâches correspondantes. Cela permet de comprendre et d'appréhender au mieux le contexte d'utilisation de ces compétences clés dites redondantes. Cela facilite ainsi l'identification des pratiques dans lesquelles ces compétences clés pourront être utilisées. Les contenus pédagogiques des formations permettant leur acquisition devront donc tenir compte autant que possible de ces caractéristiques d'application.

**Les compétences clés pour de multiples tâches**

Types de compétences	Compétences clés redondantes	Tâches associées
Savoirs	Gestion du changement	⇒ 2.3 Assurer l'adéquation entre les recommandations proposées et la mise en œuvre des solutions ⇒ 3.1 Encadrer le client dans son apprentissage des enjeux liés à la Sécurité de l'Information
	Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17999, ISO 27001)	⇒ 1.2 Comprendre les spécificités du client ⇒ 1.5 Traduire les spécificités fonctionnelles et non fonctionnelles en plans d'action, politique de sécurité, etc
	Veille technologique	⇒ 2.5 Etudier les intégrateurs, les distributeurs et les solutions du marché ⇒ 3.4 Se former aux évolutions du domaine de la Sécurité de l'Information et aux pratiques et stratégies des entreprises
Savoir être	Aisance relationnelle	⇒ 1.2 Comprendre les spécificités du client ⇒ 3.1 Encadrer le client dans son apprentissage des enjeux liés à la Sécurité de l'Information
Savoir-faire	Mettre en conformité l'organisation	⇒ 1.6 Assurer un pilotage stratégique ⇒ 2.3 Assurer l'adéquation entre les recommandations proposées et la mise en œuvre des solutions
Savoirs technologiques	Intégration de nouvelles technologies au Système d'Information existant	⇒ 2.3 Assurer l'adéquation entre les recommandations proposées et la mise en œuvre des solutions ⇒ 2.5 Etudier les intégrateurs, les distributeurs et les solutions du marché ⇒ 2.6 Evaluer les solutions proposées

Une compétence clé dite redondante interpelle. Il s'agit du savoir technologique « *Intégration de nouvelles technologies au système d'Information existant* ». Cette dernière apparaît clé pour les trois tâches de l'activité 2 du métier de Consultant qui ont été les plus impactées par le scénario d'évolution.

Les modalités d'acquisition de cette compétence devront donc impérativement retenir ces différents contextes d'utilisation associés à l'activité de collaboration au développement de la prestation en assistant la MOA et la MOE. Cette caractéristique doit permettre de mieux comprendre le contexte global d'utilisation de cette compétence et donner ainsi une meilleure visibilité au contenu pédagogique qui pourrait être mis en place pour permettre son acquisition.

La compétence clé dite redondante « Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17999, ISO 27001) » nécessite également une attention particulière. Cette compétence est clé pour deux tâches de l'activité 1. Le contenu des formations préparant à l'exercice du métier de Consultant pourrait à ce titre s'interroger pour cette compétences, s'il est nécessaire d'élargir au contexte global de l'activité 1 « Prendre en charge les enjeux et spécificités du client ».

Par ailleurs, par rapport à ces compétences clés dites redondantes, il est important de préciser que cinq d'entre elles ont obtenu les scores les plus importants pour l'une des tâches auxquelles elles sont associées.

Elles apparaissent donc d'autant plus critiques dans la pratique de cette tâche associée. Il est donc important de s'assurer que tout Consultant en Sécurité de l'Information sera en mesure de pouvoir détenir ces compétences pour les appliquer dans leur contexte, cadre d'utilisation. Il s'agit des compétences suivantes :

- ⇒ « *Gestion du changement* » pour la tâche 2.3.
- ⇒ « *Veille technologique* » pour la tâche 3.4.
- ⇒ « *Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17999, ISO 27001)* » pour la tâche 1.5.
- ⇒ « *Aisance relationnelle* » pour la tâche 1.2.
- ⇒ « *Intégration de nouvelles technologies au Système d'Information existant* » pour la tâche 2.5.

A un niveau d'analyse plus macro, il est important de signaler que les experts ont identifié le plus grand nombre de compétences clés au sein des tâches les plus impactées de l'activité 1. Cette caractéristique appuie l'idée selon laquelle c'est l'activité 1 qui devrait être la plus influencée par le scénario d'évolution pressenti par les experts. Il conviendra donc de rester vigilant à l'évolution des pratiques de cette activité.

Qui plus est, au niveau de la typologie des compétences sélectionnées comme clés, les experts prédisent une évolution forte vers les savoir-faire et les savoirs du métier. Ainsi, non seulement, un consultant en Sécurité de l'Information se devra d'avoir un solide socle de connaissances, mais en plus il semblerait que le métier au Luxembourg devra tendre également vers une optimisation de ses pratiques d'ici 2010 au regard du nombre de savoir-faire identifié comme clé. Cela devrait avoir pour conséquence d'accroître le professionnalisme demandé dans le domaine de la consultance et dans la valeur ajoutée de son expertise.

Au niveau des savoirs technologiques, il est nécessaire de préciser que les experts ont souhaité mettre en lumière, avant tout des compétences qui faciliteront sa compréhension du système d'information de l'entreprise dans laquelle il intervient. Même si cela n'est pas mentionné dans l'étude, le Consultant en fonction de l'entreprise à laquelle il appartient, et si besoin, devra être certifié auprès d'organismes internationaux et reconnu tel que l'ISC2 pour International Information Systems Security Certification Consortium pour exemple ou par des éditeurs de solutions réseaux et sécurité (Cisco, ISS, Proventia, etc).

Ci après, un tableau répartit les compétences identifiées comme clés en fonction de leur appartenance à telle ou telle typologie de compétences.

Types de compétences	Compétences clés
<b>Savoir-faire</b>	Animer et préparer des réunions
	Connaître l'environnement technique, comprendre les solutions proposées à travers le langage commercial
	Effectuer une veille concurrentielle
	Identifier les besoins en connaissance du client
	Identifier la taille/nature/complexité de l'organisation analysée et prendre en compte des données stratégiques de l'entreprise
	Mettre en conformité l'organisation
	Réaliser des études d'impacts, des études de marché (fournisseurs)
	Réaliser l'évaluation d'une situation, d'un avancement
	Réaliser un diagnostic des besoins et analyser l'existant
<b>Savoir</b>	Valider une solution informatique ou organisationnelle en Sécurité
	Fonctionnement des organisations
	Gestion du Changement
	Gestion et conduite de projet
	Méthodes de gestion et d'analyse des risques ( Ebios, Mehari, Marion, Melisa, Cramm, Octave, etc)
	Normes et procédures de sécurité IT
	Normes professionnelles (IA, ISACA, etc)
	Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001)
	Processus business
<b>Savoir être</b>	Stratégie d'entreprise
	Veille technologique
	Aisance relationnelle
<b>Savoir technologique</b>	Ouvert d'esprit
	Rigoureux – Méthodique
	Architecture des réseaux informatiques et télécoms
Intégration de nouvelles technologies au Système d'Information existant	
Environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données, etc)	

L'ensemble des compétences citées, sont donc apparues essentielles pour les experts parmi les compétences existantes du Consultant à horizon 2010.

Pour autant, le référentiel initial du métier étudié ne peut être exhaustif. Ainsi, il est intéressant de poursuivre la réflexion pour savoir si de nouvelles compétences doivent être envisagées dans la pratique du métier. C'est l'objet de la partie suivante.

### 3. Les compétences nouvelles pour le Consultant en Sécurité de l'Information

La réflexion des experts a abouti à la détection des compétences actuelles qui seront essentielles dans l'exercice du métier de Consultant en Sécurité de l'Information à l'horizon 2010. Afin de compléter cette réflexion, les experts ont identifié quelles seront les compétences nouvelles et éléments nouveaux du métier à horizon 2010. Ils ont ainsi identifié **sept compétences nouvelles** au regard du profil professionnel existant du métier étudié. (tableau récapitulatif des compétences nouvelles page suivante)

Ces compétences nouvelles ont été identifiées à partir du constat suivant.

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. Son rôle d'assistant à la MOA par rapport à un MOE devrait s'accroître selon les experts. A ce titre, il devra être en mesure d'aligner au mieux les besoins de sécurité de l'organisation avec les solutions de sécurité proposées. Les réflexions et justifications faites au client, devront donc être mieux argumentées et structurées pour permettre au client d'avoir une meilleure visibilité sur les choix qui s'offrent à lui.

Par ailleurs, les experts ont envisagé à terme qu'il y ait deux profils de consultant dans le domaine de la Sécurité de l'information ; d'une part des professionnels spécialisés au niveau des aspects techniques et d'autre part, des consultants orientés sur les problématiques organisationnelles en matière de sécurisation de l'information. Pour ces derniers, les experts estiment que cette pratique de la consultance ne pourra être faite que par des professionnels aguerris, ayant le bagage nécessaire pour appréhender la complexité de la dynamique organisationnelle dans laquelle il intervient.

Toutefois, quelque 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. Une meilleure compréhension du contexte dans lequel il intervient, lui sera demandé. Il lui faudra alors personnaliser autant que possible les solutions proposées qu'elles soient, de nature technique et/ou organisationnelle.

## Les compétences nouvelles pour le Consultant en Sécurité de l'Information

Types de compétences	Éléments nouveaux exprimés	Synthèse des commentaires justificatifs exprimés par les experts
<b>Savoir-faire</b>	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)	I 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
<b>Savoir-être</b>	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

#### 4. Canevas d'investigation à l'attention des organismes de formation

A partir des informations fournies préalablement, une première série de questions doivent être posée pour faciliter la constitution ou l'adaptation de modules de formation, adaptés au métier de Consultant en Sécurité de l'information.

- Quelles sont les compétences clés considérées comme les **pré-recquis** à l'exercice du métier de Consultant en Sécurité de l'information?
- Quelles sont les compétences clés **transverses** à plusieurs activités du métier et qui risquent d'être nécessaires de manière continue à la réalisation de multiples tâches du métier ?
- Quelles sont les compétences clés **spécifiques à une seule activité** du métier de Consultant en Sécurité de l'Information ?
- Quelles sont les compétences clés qui sont **spécifiques à une tâche** et donc à un contexte d'utilisation ?
- Quelles sont les compétences clés qui sont apparues **critiques** pour la réalisation d'une ou plusieurs tâches de par les résultats des évaluations des experts?
- A quel **contexte d'utilisation (activités/tâches)**, est-il possible d'associer les **compétences nouvelles** ?

Ces questions ne sont pas exhaustives. Elles cherchent avant tout à proposer une aide à la décision pour établir le profil de formation du métier de Consultant en Sécurité de l'Information qui soit le plus adéquat aux changements dont le métier en question va devoir faire face à horizon 2010.

Le cadre d'exigence de mise en œuvre de ces compétences, étant précisé, il appartiendra aux organismes de formation intéressés par les résultats de proposer ou non des contenus pédagogiques qui facilitent l'appropriation de ces compétences. Pour élaborer de manière concrète ces contenus pédagogiques, une deuxième série de questions<sup>4</sup> repères peuvent permettre aux organismes de formation de déterminer jusqu'où ils souhaitent tendre dans l'acquisition de ces compétences.

- N'y a-t-il pas des nuances ou des degrés de maîtrise de certaines compétences qu'il serait nécessaire de préciser en fonction des modules de formation?
- Quelles sont les compétences requises auxquelles vous pensez que les organismes de formation peuvent apporter une réponse exclusive ? ...Non-exclusive ? ...Aucune réponse (apprentissage par l'action en entreprise, sur le tas) ?
- Quelle est la méthode pédagogique utilisée pour acquérir la compétence « X » ? (stage, atelier, exposé, ...).
- Est-ce nécessaire d'avoir un pré-requis pour acquérir la compétence « X » ? Si oui, lequel ?
- Au sein de votre offre de formation, quelle(s) compétence(s) nouvelle(s) peut être rapprocher/intégrer au sein d'un enseignement que vous êtes déjà amené à proposer ?
- Au regard des compétences clés et nouvelles qui seront nécessaires à l'horizon 2010, dans quelle direction votre institution devrait s'orienter en matière de politique pédagogique ?

---

<sup>4</sup> Ces questions sont extraites du guide utilisateur de la démarche d'anticipation des compétences, disponible sur le site [www.abilitic.eu](http://www.abilitic.eu)

## Conclusion

Il a été possible à travers l'étude menée sur le devenir de Consultant en Sécurité de l'information d'identifier quels seront les futurs besoins en matière de compétences pour exercer ce métier au Luxembourg à horizon 2010.

Il est important pour finir de mettre en relation les résultats des travaux menés sur le devenir du métier étudié avec les conclusions principales de l'édition 2007 de l'enquête intitulée "Global State of Information Security Survey" menée conjointement par PricewaterhouseCoopers et les magazines CIO et CSO<sup>5</sup>. En effet, un bilan mitigé ressort en matière de mise en place et de surveillance des politiques de sécurité au niveau international, Luxembourg compris. Si les entreprises ont tendance selon cette étude à investir dans les infrastructures informatiques, elles restent souvent à la traîne en matière de mise en oeuvre, d'évaluation et d'examen des politiques liées à la sécurité et à la confidentialité des informations transmises.

Or qui mieux que le Consultant en Sécurité de l'Information peut apporter une expertise dans l'aide à la mise en oeuvre des bonnes pratiques en matière de Sécurité. Le niveau de sécurité requis apparaissant de plus en plus important, il devient nécessaire de peser le pour et le contre des éventuels compromis entre sécurité optimale du Système d'Information et des applications d'un côté, et couverture des besoins utilisateurs de l'autre. La focalisation que les experts ayant participé à la démarche d'anticipation, ont fait notamment sur les tâches de l'activité liée à la prise en charge des enjeux et spécificités du client, doit permettre d'y répondre au mieux.

Pour autant, le Consultant en Sécurité de l'Information ne devra pas sous estimer ses savoir-être et aptitudes relationnelles. Ils lui permettront de faire face aux situations critiques auxquelles il sera nécessairement confronté.

Les résultats de l'étude doivent donc être appréhendés comme des pistes d'investigation. Ils doivent faciliter autant que possible l'adaptation des programmes de formation au plus près des revendications des professionnels qui exercent ou ont exercé, la fonction de Consultant en Sécurité de l'Information.

---

<sup>5</sup> L'étude intitulée "Global State of Information Security Survey 2007" est disponible sur le site [www.pwc.com/giss2007](http://www.pwc.com/giss2007)

## Références

- Hua D, Meunier B, Girard F, Durand A (2007) « La Sécurité de l'Information au Grand Duché du Luxembourg en 2010 ? », 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.
- Etude menée conjointement par PricewaterhouseCoopers et les magazines CIO et CSO : "Global State of Information Security Survey 2007"