

Anticipation des compétences du métier d'Auditeur en Sécurité de l'Information à horizon 2010

Résumé

Le présent document expose le résultat d'une réflexion structurée, menée par **14 professionnels du domaine de la Sécurité de l'Information** qui se sont attachés à **analyser l'évolution spécifique du métier d'Auditeur 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, **une dizaine de compétences nouvelles a été recensée.**

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

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 Meunier¹, Duan Hua², Alex Durand³, Frédéric Girard⁴

¹bertrand.meunier@tudor.lu - Chef de projet R&D

²duan.hua@tudor.lu - Expert méthode

³alex.durand@tudor.lu - Coordinateur Scientifique

⁴frederic.girard@tudor.lu - Reviewer

www.citi.tudor.lu

Remerciements

L'équipe du projet Abilitic¹ adresse ses remerciements à :

- Monsieur BONBARDELLA Roland (Haut Commissariat à la Protection Nationale)
- Madame FRAN CART Sylviane (FORTIS Banque Luxembourg)
- Monsieur HAGEN David (Commission de Surveillance du Secteur Financier)
- Monsieur HUMBERT Jean - Philippe (Office Luxembourgeois d'Accréditation et de Surveillance)
- Monsieur MAYER Nicolas (CRP Henri TUDOR)
- Madame MULLER Clara (P&T)
- Madame PELTIER Noëlle (CRP Henri TUDOR)
- Monsieur POGGI Sébastien (CRP Henri TUDOR)
- Monsieur ROSEVEGUE Alexandre (BNP Parisbas)
- Monsieur TAMISIER Thomas (Centre de Recherche Public Gabriel LIPPMANN)
- Madame THIEL Florence (Crédit Agricole)
- Monsieur THILL François (Ministère de l'Economie et du Commerce Extérieur Luxembourgeois)
- Monsieur WEIMERSKIRCH Pierre (Commission Nationale pour la Protection des Données)
- Monsieur VAN DAMME Johan (European Court of Auditors)

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

¹ 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

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 d'Auditeur en Sécurité de l'Information	8
4. Les Compétences principales du métier	9
III. Phase n°2 : Le profil d'évolution du métier d'Auditeur 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 tâches du métier impactées par le changement	16
2. Les compétences clés de l'Auditeur en Sécurité de l'Information	18
3. Les compétences nouvelles pour l'Auditeur en Sécurité de l'Information	26
4. Les orientations à investiguer par les organismes de formation.....	28
Conclusion.....	31
Références	32

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 d'Auditeur 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 documenté². 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 d'Auditeur 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 d'Auditeur 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 Auditeur en Sécurité de l'Information devra maîtriser demain dans l'exercice de sa fonction.

² 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 d'Auditeur 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 d'Auditeur 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 d'Auditeur en Sécurité de l'Information est présenté en termes **d'activité, de tâche et de compétence**. 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 d'Auditeur en Sécurité de l'Information étant conséquent, il est disponible sur le site 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 du 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 d'Auditeur 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 l'auditeur en Sécurité de l'information a été défini de la manière suivante. Il a ainsi pour fonction 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.**

Le choix a été fait dans l'étude du devenir de ce métier de l'appréhender à la fois comme un métier pouvant s'exercer en appartenant à un département interne d'une entreprise mais également, comme un prestataire, intervenant extérieur. Lors du travail de formalisation, de définition des compétences attendues du métier d'auditeur en Sécurité de l'Information, il a donc fallu tenir compte de cette dualité. C'est pourquoi, le champ des prérogatives définies pour ce métier peut paraître extrêmement large. Par ailleurs, les activités de ce métier ont été définies, de telle sorte à ce que ses actions en tant qu'Auditeur en Sécurité de l'Information aient un impact, une influence 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 :

- Contextualiser la mission d'audit,
- Dérouler la mission d'audit,
- Orchestrer et développer la communication envers le(s) commanditaire(s) de l'Audit et les audités,
- Manager une équipe d'audit,
- S'intégrer dans une équipe d'audit.

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

Par ailleurs, une activité de communication à part entière a été identifiée pour les prérogatives du métier d'Auditeur en Sécurité de l'Information. En effet, les experts qui ont participé à la définition du métier, ont souhaité mettre en avant l'intérêt de faire valoir ce type d'activité pour que l'Auditeur dans l'exécution de ses missions, la présentation de ses travaux, soit mieux compris, interprété et accepté au sein de l'organisation.

Enfin, deux activités périphériques ont également été associées au métier d'Auditeur en Sécurité de l'information. Il s'agit d'une activité de management d'une équipe d'Audit ainsi que d'une activité liée à sa capacité à s'intégrer dans une équipe d'audit. Dans le cadre de ces deux activités, des actions précises doivent être appréhendées par l'Auditeur en Sécurité de l'Information pour lui permettre de bien se positionner lors du déroulement de sa mission d'Audit.

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 d'Auditeur en Sécurité de l'Information aujourd'hui.

Au niveau des savoirs technologiques, il ne s'agit pas pour l'Auditeur en Sécurité de l'Information de maîtriser ou d'être expert dans l'utilisation et l'exploitation des compétences identifiées, il s'agit pour lui de comprendre au mieux les systèmes d'information mises en place au sein d'une entreprise et de vérifier sa conformité ou non par rapport à un référentiel donné.

3. Activités et tâches associés du métier d'Auditeur en Sécurité de l'Information

<p><u>Activité 1 : Contextualiser la mission d'audit</u></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><u>Activité 2 : Dérouler la mission d'audit</u></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><u>Activité 3 : Orchestrer et développer la communication envers le(s) commanditaires de l'audit et les audités</u></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><u>Activité 4 : Manager une équipe d'audit</u></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><u>Activité 5 : S'intégrer dans une équipe</u></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 	

4. Les Compétences principales du métier

<p style="text-align: center;"><u>Savoirs</u></p>	<p style="text-align: center;"><u>Savoir-être</u></p>
<p style="text-align: center;"><u>Savoir-faire</u></p> <ul style="list-style-type: none"> • Tenir à jour les templates communs d'audit • Rédiger ou participer à la rédaction d'une lettre de mission • 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 • Faire évoluer le questionnaire d'Audit • Dialoguer - interroger - interviewer des collaborateurs • Effectuer des réunions d'ouverture et de clôture d'audit • Demander l'accès aux documents pertinents • Effectuer la collecte des données et l'agrégation des données • Mettre en oeuvre une analyse des risques • 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 • Planifier et ordonnancer des audits • 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 • Valider des constats d'action avec le ou les responsables de l'entité auditée • Se tenir informé des évolutions réglementaires, du référentiel de base, des normes, standards et du contexte de l'entreprise • Alerter la hiérarchie en cas de problèmes majeurs • Se soucier de la qualité de service au client 	<p style="text-align: center;"><u>Savoirs technologiques</u></p> <ul style="list-style-type: none"> • Architecture fonctionnelle du SI (Système d'Information) de l'entreprise (logiciels, application métiers) • Environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données, etc) • Architecture de systèmes d'exploitation • Architecture des réseaux informatiques et télécoms • Architecture technique du SI de l'entreprise • Intégration de nouvelles technologies au SI • Intégration de systèmes d'exploitation • Droits d'accès aux applications et services • Développement d'algorithmique • Protocole de communication

III. Phase n°2 : Le profil d'évolution du métier d'Auditeur 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 d'Auditeur en Sécurité de l'Information. Pour connaître ses modalités d'élaboration, un rapport³ documenté sur l'ensemble des étapes ayant permis sa construction est disponible sur le site : www.abilitic.eu.

N°	Intitulés des facteurs d'évolution essentiels	Hypothèses d'évolution retenues
1	<i>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
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

³ 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 luxembourgeoise. 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 de 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 d'Auditeur 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 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 à proposer des pistes d'investigation pour orienter les organismes de formation dans l'élaboration d'un programme répondant aux défis à venir du métier d'Auditeur en Sécurité de l'Information.

1. Les 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 d'Auditeur 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 **sept tâches ont été sélectionnées et considérées comme susceptibles d'évoluer fortement face au changement.**

Au regard de la mesure d'impact du scénario d'évolution sur le profil professionnel du métier d'Auditeur en Sécurité de l'Information, il apparaît que **les activités 1 et 2, respectivement liés à la contextualisation et au déroulement de la mission d'audit ont été les plus impactées par le scénario d'évolution du domaine de la Sécurité de l'Information. 2 et 3 tâches pour chacune des activités respectives cités ont été impactées.**

Pour l'activité 1 : Contextualiser la mission d'audit	Pour l'activité 2 : Dérouler la mission d'audit
<ul style="list-style-type: none"> - 1.1 Mettre à jour ses connaissances pour la réalisation de l'audit - 1.2 Analyser le scope de la mission 	<ul style="list-style-type: none"> - 2.1 Réaliser des interviews et des entretiens - 2.2 Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre) - 2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel

Selon les experts, et au regard des changements annoncés, l'Auditeur en Sécurité de l'Information devra porter une attention particulière à la mise à jour de ses connaissances au regard du contexte organisationnel, culturel et business de l'entreprise dans laquelle il interviendra. Ce travail de mise à jour lui permettra alors d'être à même de cerner au mieux le scope de sa mission et son champ d'intervention.

Pour le déroulement même de la mission d'audit, une mise en avant des capacités de recueil d'informations a été faite par les experts ayant participé à la démarche d'anticipation des compétences. Que cela soit dans la réalisation des interviews, des entretiens, dans le contrôle des applications et des personnes, l'Auditeur en Sécurité de l'Information devra tâcher d'identifier et sélectionner les informations les plus pertinentes à sa mission. Pour autant, il ne lui faudra pas occulter les limites de son travail au regard du périmètre d'analyse et du référentiel d'audit choisi. Cela lui pourrait lui permettre d'appuyer encore davantage les apports de son analyse.

Deux autres tâches seront, semble t il fortement évolutives dans les années à venir au regard des changements pressentis. Il s'agit des tâches « 4.4. Standardiser les méthodes de travail (approche commune) » et « 5.4 Communiquer avec les autres fonctions de contrôle. ». Il s'agit de deux tâches qualifiées de périphériques au cœur de métier d'un Auditeur en Sécurité de l'Information.

Pour finir, il est à noter que les tâches de l'activité 3 liées à l'orchestration et au développement de la communication envers le(s) commanditaires de l'audit et les audités, n'ont pas été vues comme étant les plus fortement évolutives au regard des changements pressentis d'ici 2010 pour le domaine de la sécurité de l'Information.

A la lecture des différents tableaux proposés ci-après (point 2), **l'activité 1** du métier d'Auditeur en Sécurité de l'Information « **contextualiser la mission d'audit** », apparaît être celle qui sera la plus impactée par le scénario d'évolution identifié à horizon 2010. 6 changements ont été sélectionnés par les experts comme pouvant fortement influencer le devenir de la pratique des tâches associées à cette activité. Toutefois il faut reconnaître que cet impact n'est pas homogène pour les tâches retenues. En effet, la tâche « **1.1 Mettre à jour ses connaissances** » est fortement impactée puisque 5 changements auront semblent - ils une influence sur l'importance et la nécessité de la maîtriser pour exercer le métier étudié.

L'impact par contre des changements composant le scénario d'évolution du domaine de la Sécurité de l'Information sur **l'activité 2** « **Dérouler la mission d'Audit** » apparaît pour sa part plus équilibré. 4 changements ont été identifiés comme pouvant influencer la pratique et le devenir des tâches associées retenues lors de l'évaluation des experts. Sur ces 4 changements, 2 apparaissent à plusieurs reprises comme étant déterminantes dans la réalisation des tâches sélectionnées par les experts. Il appartiendra donc aux Auditeurs en Sécurité de l'Information de veiller notamment à l'avènement ou non de ces deux changements :

- « En 2010 l'intégration du Risk Management sera plus homogène grâce à la promotion du RM et à la prise de conscience des entreprises »
- « En 2010, il y aura une prise en compte de la sécurité lors de la conception des technologies. (Privacy Enhanced Technology). »

Il est à noter à ce titre que le changement lié à l'intégration plus homogène du Risk Management au sein des entreprises semble déterminant dans l'évolution des pratiques du métier d'Auditeur en Sécurité de l'Information. Il est en effet apparu de nouveau lors des évaluations des experts comme déterminant dans l'évolution de la pratique de la tâche « **4.4 Standardiser les méthodes de travail (approche commune)** » de l'activité 4 « Manager une équipe d'audit ».

Par ailleurs, il est nécessaire de suivre avec attention le devenir du changement lié à la convergence entre les domaines de la qualité et de la sécurité de l'information grâce à l'intégration des questions de sécurité dans les normes qualité (ISO). Ce changement, s'il est avéré, impactera la pratique en effet de deux tâches ; « 1.1 Mettre à jour ses connaissances » et « 4.4. Standardiser les méthodes de travail (approche commune) ».

En approfondissant l'analyse sur les tâches même du métier, il est important de mettre en avant les deux tâches qui seraient les plus impactées par le scénario d'évolution sélectionné.

- « **1.1. Mettre à jour ses connaissances** » dans l'activité 1 « Contextualiser la mission d'audit ». Cette tâche est impactée fortement par 5 changements d'ordre politique, technologique et socio culturel.
- « **2.5. Identifier les forces et faiblesses du périmètre d'analyse** » dans l'activité 2 « Dérouler la mission d'audit ». Cette tâche sera impactée par 3 changements d'ordre législatif et organisationnel dans le domaine de la Sécurité de l'Information.

La tâche « **2.2 Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre)** » pour l'activité 2 « Dérouler la mission d'audit » ainsi que la tâche « **4.4. Standardiser les méthodes de travail (approche commune)** » pour l'activité 4 « Manager une équipe d'Audit » seraient aussi confrontées à l'influence de changements multiples. Ces deux dernières tâches seraient toutefois impactées dans une moindre mesure que les deux tâches citées précédemment. 2 changements au maximum impacteraient leur réalisation

Pour chacune de ses tâches, l'Auditeur en Sécurité de l'Information se devra d'être vigilant à l'avènement ou non des changements associés. Ces derniers influenceront fortement son employabilité sur le marché Grand Ducal.

2. Les compétences clés de l'Auditeur 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 ayant eu le nombre de points le plus élevés par tâches lors des évaluations des experts⁴, sont mises en évidence par un fond bleu.

Pour l'activité 1 : Contextualiser la mission d'Audit

Scénario d'évolution	Tâches	Compétences Clés
<i>En 2010, émergence d'une entité d'assistance (CERT) au GDL.</i>	1.1 Mettre à jour ses connaissances	Normes professionnelles d'audit (IA, ISACA, ...)
<i>En 2010, l'impact d'éventuelles catastrophes numériques sera réduit grâce à une amélioration de l'analyse des risques et de la gestion des crises. (multiplication des procédures et des tests de fiabilité des systèmes)</i>		Se tenir informé des évolutions réglementaires, du référentiel de base, des normes, standards et du contexte de l'entreprise
<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>		Méthodes de gestion et d'analyse de risques (Équation du risque, Ebios, Mehari, Marion, Callio, Melisa, Cramm, Octave...)
<i>En 2010, il y aura une convergence de la qualité/sécurité grâce à l'intégration de la sécurité dans les normes qualité. (ISO)</i>		Environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données...)
<i>En 2010 la criticité des SIC sera de plus en plus importante au même titre que des ressources primaires(eau électricité) : forte dépendance</i>		Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001)
		Intégration de nouvelles technologies au SI
		Gestion des compétences
		Processus business
<i>En 2010, les autorités administratives et réglementaires imposeront la mise en place d'un niveau de sécurité minimum et/ou certaines règles de sécurité aux entreprises de certains secteurs (ex: secteur financier) secteurs régulés</i>	1.2 Analyser le scope de la mission	Analyser de l'information technique et organisationnelle (revue de procédures internes, historique de l'entreprise) Processus business
		Normes spécifiques au métier de l'entreprise audité
		Se tenir informé des évolutions réglementaires, du référentiel de base, des normes, standards et du contexte de l'entreprise
		Stratégie d'entreprise
		Analyste
		Définir l'objectif et le programme d'audit correspondant
	Identifier et prendre en compte des données stratégiques de l'application de normes et de standards	

⁴ Question posée aux experts présents lors de l'atelier : Veuillez indiquer quelles sont les compétences essentielles pour la réalisation de chacune de ces tâches ?

Pour l'activité 2 : Dérouler la mission d'audit

Scénario d'évolution	Tâches	Compétences Clés
<p><i>En 2010 l'intégration du Risk Management sera plus homogène grâce à la promotion du RM et à la prise de conscience des entreprises.</i></p>	<p>2.1 Réaliser des entretiens et des interviews</p>	<p>Dialoguer – interroger - interviewer des collaborateurs Elaborer un questionnaire d'audit Techniques d'entretien propres à l'audit Ouvert d'esprit - Curieux Effectuer la collecte et l'agrégation des données Diplomate - aisance relationnelle Architecture fonctionnelle du SI de l'entreprise (logiciels, applications métiers) Architecture technique du SI de l'entreprise Environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données...) Observateur – discret</p>
<p><i>En 2010 l'auto régulation et la mise en place de codes de bonne conduite va impliquer les ISP dans la sécurité de l'information.</i></p> <p><i>En 2010, il y aura une prise en compte de la sécurité lors de la conception des technologies. (Privacy Enhanced Technology).</i></p>	<p>2.2 Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre)</p>	<p>Faire un audit de l'architecture réseau, des procédures d'exploitation, du logiciel serveur, du matériel, du système d'exploitation Effectuer la collecte et l'agrégation des données Concepts et pratiques d'audit Analyste Droits d'accès aux applications et services Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001) Normes et procédures de sécurité IT</p>
<p><i>En 2010, les autorités administratives et réglementaires imposeront la mise en place d'un niveau de sécurité minimum et/ou certaines règles de sécurité aux entreprises de certains secteurs (ex: secteur financier) secteurs régulés</i></p>	<p>2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel</p>	<p>Analyser de l'information technique et organisationnelle (revue de procédures internes, historique de l'entreprise)</p> <p>Mettre en place des indicateurs afin de s'assurer de l'application de normes et standards</p> <p>Normes et procédures de sécurité IT Analyste</p>
<p><i>En 2010 l'intégration du Risk Management sera plus homogène grâce à la promotion du RM et à la prise de conscience des entreprises.</i></p> <p><i>En 2010, il y aura une prise en compte de la sécurité lors de la conception des technologies. (Privacy Enhanced Technology).</i></p>		<p>Environnement général du SI de l'entreprise (environnements d'exploitation de l'ERP, base de données...)</p> <p>Faire un audit de l'architecture réseau, des procédures d'exploitation, du logiciel serveur, du matériel, du système d'exploitation</p> <p>Méthodes de gestion et d'analyse de risques (Equation du risque, Ebios, Mehari, Marion, Callio, Melisa, Cramm, Octave...)</p> <p>Processus business</p>

Pour l'activité 4 : Manager une équipe

Scénario d'évolution	Tâches	Compétences Clés
<i>En 2010, il y aura une convergence de la qualité/sécurité grâce à l'intégration de la sécurité dans les normes qualité. (ISO)</i> <i>En 2010 l'intégration du Risk Management sera plus homogène grâce à la promotion du RM et à la prise de conscience des entreprises..</i>	4.4. Standardiser les méthodes de travail (approche commune)	Normes professionnelles d'audit (IA, ISACA...)
		Mettre en place des indicateurs afin de s'assurer de l'application de normes et standards Concepts et pratiques d'audit Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001)

Pour l'activité 5 : Communiquer avec les autres fonctions de contrôle

Scénario d'évolution	Tâches	Compétences Clés
<i>En 2010, les pouvoirs publics et les associations intensifieront la sensibilisation à la SI. (multiplication des cibles)</i>	5.4. Communiquer avec les autres fonctions de contrôle	Réaliser des supports d'informations sur le déroulement de l'audit Rigoureux-Méthodique
		Travail en équipe
		Intègre
		Diplomate-Aisance relationnelle
		Concepts et pratiques d'audit
		Processus business

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

Tout d'abord, il apparaît intéressant de signaler que certaines compétences clés le sont, pour plusieurs tâches d'une même activité ou d'activités différentes. 14 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 peuvent être utilisées. Les contenus pédagogiques des formations permettant l'acquisition de ces compétences devront donc tenir compte autant que possible de ces caractéristiques. Une dominance de savoirs et savoir-faire se constate au niveau des compétences clés les plus récurrentes.

Les compétences clés pour de multiples tâches

Types de compétences	Compétences clés redondantes	Tâches associées
Savoir	Concepts et pratiques d'audit	⇒ 2.2 Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre) ⇒ 4.4. Standardiser les méthodes de travail (approche commune) ⇒ 5.4 Communiquer avec les autres fonctions de contrôle
	Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001)	⇒ 1.1 Mettre à jour ses connaissances ⇒ 2.2 Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre) ⇒ 4.4. Standardiser les méthodes de travail (approche commune)
	Normes professionnelles d'audit (IA, ISACA...)	⇒ 1.1 Mettre à jour ses connaissances ⇒ 4.4. Standardiser les méthodes de travail (approche commune)
	Normes et procédures de sécurité IT	⇒ 2.2 Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre) ⇒ 2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel
	Processus business	⇒ 1.1 Mettre à jour ses connaissances ⇒ 2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel ⇒ 5.4. Communiquer avec les autres fonctions de contrôle
	Méthode de gestion et d'analyse des risques (Equation du risque, Ebios, Mehari, Marion, Callio, Melisa, Cramm, Octave, etc)	⇒ 1.1 Mettre à jour ses connaissances ⇒ 2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel
Savoir être	Analyste	⇒ 1.1 Analyser le scope de la mission ⇒ 2.2 Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre) ⇒ 2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel
	Diplomate aisance relationnelle	⇒ 2.1 Réaliser des entretiens et des interviews ⇒ 5.4. Communiquer avec les autres fonctions de contrôle
Savoir-faire	Analyser de l'information technique et organisationnelle (revue de procédures internes, historique de l'entreprise)	⇒ 1.2 Analyser le scope de la mission ⇒ 2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel
	Effectuer la collecte des données et l'agrégation des données	⇒ 2.1 Réaliser des entretiens et des interviews ⇒ 2.2 Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre)
	Faire un audit de l'architecture réseau, des procédures d'exploitation, du logiciel serveur, du matériel, du système d'exploitation	⇒ 2.2 Rechercher des preuves et des évidences en contrôlant les applications et personnes (procédures mises en œuvre) ⇒ 2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel
	Mettre en place des indicateurs afin de s'assurer de l'application de normes et standards	⇒ 2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel ⇒ 4.4. Standardiser les méthodes de travail (approche commune)
	Se tenir informé des évolutions des évolutions réglementaires, du référentiel de base, des normes, standards et du contexte de l'entreprise	⇒ 1.1 Mettre à jour ses connaissances ⇒ 1.2 Analyser le scope de la mission
Savoir technologique	Environnement général du SI de l'entreprise (environnement d'exploitation de l'ERP, base de données, etc)	⇒ 1.1 Mettre à jour ses connaissances ⇒ 2.1 Réaliser des entretiens et des interviews ⇒ 2.5 Identifier les forces et faiblesses du périmètre d'analyse et du référentiel

3 compétences clés dites redondantes ont une caractéristique commune. Elles ont obtenu pour chacune des tâches auxquelles elles sont associées les scores les plus importants. Elles apparaissent donc d'autant plus critiques dans la pratique des tâches associées. Il est donc important de s'assurer que tout Auditeur en Sécurité de l'Information est en mesure de pouvoir détenir ces compétences et les appliquer dans leur contexte, cadre d'utilisation. Il s'agit de deux savoir-faire et d'un savoir :

- ⇒ « **Analyser de l'information technique et organisationnelle (revue de procédures internes, historique de l'entreprise) »**
- ⇒ « **Mettre en place des indicateurs afin de s'assurer de l'application de normes et standards »**
- ⇒ « **Normes professionnelles d'audit (IA, ISACA...) »**

Qui plus est, il est important de souligner que 3 compétences sont clés pour des tâches appartenant à une même activité. Cette caractéristique permet de mieux comprendre le contexte global d'utilisation de ces compétences et de donner une visibilité au contenu pédagogique qui pourrait être mis en place pour permettre leur acquisition.

Pour l'activité 1 :

- ⇒ « **Se tenir informé des évolutions réglementaires, du référentiel de base, des normes, standards et du contexte de l'entreprise »**

Pour l'activité 2.

- ⇒ « **Effectuer la collecte des données et l'agrégation des données »**,
- ⇒ « **Faire un audit de l'architecture réseau, des procédures d'exploitation, du logiciel serveur, du matériel, du système d'exploitation »**,
- ⇒ « **Normes et procédures de sécurité IT »**

Il est également utile de faire mention de manière explicite aux compétences clés qui sont associées à de multiples tâches dans des activités différentes (au minimum 3). Cela illustre le caractère transverse de ces compétences et l'utilité de s'interroger si ces compétences sont présentes dans le socle de connaissances de base d'une formation pour un Auditeur en Sécurité de l'Information. Il s'agit des trois savoirs suivants :

- ⇒ **Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001)**
- ⇒ **Concepts et pratiques d'audit**
- ⇒ **Processus business**

Il faut toutefois préciser que ces compétences si elles sont clés pour chacune des tâches sélectionnées, n'ont pas recueilli les scores les plus importants (excepté pour le savoir « processus business » dans la tâche 1.1) lors des évaluations des experts.

A ce titre, il est rappelé dans le tableau ci après l'ensemble des compétences qui ont recueilli les scores les plus importants lors des évaluations des experts. Il est fait mention de compétences clés considérées comme étant les plus déterminantes.

Les compétences clés les plus déterminantes

Savoirs	Méthodes de gestion et d'analyse de risques (Équation du risque, Ebios, Mehari, Marion, Callio, Melisa, Cramm, Octave...)
	Normes professionnelles d'audit (IA, ISACA, ...)
	Processus business
	Techniques d'entretien propres à l'audit
Savoir-être	Ouvert d'esprit – Curieux
	Rigoureux-Méthodique
Savoir- faire	Analyser de l'information technique et organisationnelle (revue de procédures internes, historique de l'entreprise)
	Dialoguer - interroger - interviewer des collaborateurs
	Effectuer la collecte et l'agrégation des données
	Elaborer un questionnaire d'audit
	Faire un audit de l'architecture réseau, des procédures d'exploitation, du logiciel serveur, du matériel, du système d'exploitation
	Mettre en place des indicateurs afin de s'assurer de l'application de normes et standards (2)
	Réaliser 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

Cela permet au-delà des compétences clés qui ont déjà été mises en avant, d'insister sur des besoins spécifiques pour l'Auditeur en Sécurité de l'Information en matière de formation.

Ainsi, parmi les compétences clés qui n'ont pas encore été citées, de multiples compétences liées à ses capacités d'animation d'entretiens, d'interviews ainsi que de communication envers les autres fonctions de contrôle en entreprise complètent les analyses préalables :

- ⇒ **Elaborer un questionnaire d'audit**
- ⇒ **Techniques d'entretiens propres à l'audit**
- ⇒ **Dialoguer - interroger - interviewer des collaborateurs**
- ⇒ **Ouvert d'esprit – Curieux**
- ⇒ **Réaliser des supports d'informations sur le déroulement de l'audit**
- ⇒ **Rigoureux méthodique**

Il est donc utile et important de croiser les différentes analyses pour permettre l'identification la plus pertinente possible des compétences à acquérir, à détenir pour 2010 pour ce métier.

Dans le tableau qui suit, ci après, les compétences clés présentées sont celles que les experts ayant participé à la démarche d'anticipation des compétences ont souhaité mettre avant en priorité pour le métier étudié. Ces compétences ont donc été retenues suite aux différents exercices proposés dans le cadre de la démarche d'anticipation des compétences.

Il s'agit des compétences clés les plus significatives selon les experts parmi celles qui sont transverses, spécifiques ainsi que celles ayant obtenues les scores les plus élevés lors des différentes évaluations.

Compétences clés retenues pour la pratique du métier étudié

Savoirs	Méthodes de gestion et d'analyse de risques (Équation du risque, Ebios, Mehari, Marion, Callio, Melisa, Cramm, Octave...)
	Normes et procédures de sécurité IT
	Normes professionnelles d'audit (IA, ISACA, ...)
	Normes, méthodes, outils et référentiels qualité sécurité (ITIL, ISO 17799, ISO 27001) (3)
	Processus business
	Techniques d'entretien propres à l'audit
Savoir-faire	Analyser de l'information technique et organisationnelle (revue de procédures internes, historique de l'entreprise)
	Définir l'objectif et le programme d'audit correspondant
	Dialoguer - interroger - interviewer des collaborateurs
	Effectuer la collecte et l'agrégation des données
	Elaborer un questionnaire d'audit
	Faire un audit de l'architecture réseau, des procédures d'exploitation, du logiciel serveur, du matériel, du système d'exploitation
	Identifier et prendre en compte des données stratégiques de l'application de normes et de standards
	Mettre en place des indicateurs afin de s'assurer de l'application de normes et standards
Savoir technologique	Réaliser 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
Savoir technologique	Intégration de nouvelles technologies au Système d'Information

Au regard des changements identifiés pour le devenir du domaine de la Sécurité de l'Information au Luxembourg à horizon 2010, un besoin fort se constate dans la maîtrise avant tout, de savoir-faire et donc, de pratiques homogènes, matures pour la mise en oeuvre de ces savoir-faire.

Les savoir être ont été supprimé en définitive dans le choix des compétences clés à mettre en avant. Ces savoir-être sont apparus pour les experts implicites dans la pratique du métier. Sans ces caractéristiques intrasèques à la fois de curiosité, et de rigueur (savoir-être dits les plus déterminants) mais également d'aisance relationnelle en public et de capacité d'analyse (savoir-être dits redondants), un individu ne pourrait de toute manière exercer à terme la fonction d'Auditeur en Sécurité de l'Information. Il s'agit davantage pour les experts de prérequis de base qui seront quoiqu'il adienne toujours nécessaires à la pratique du métier d'Auditeur en Sécurité de l'Information et ce, quelque soit l'évolution du métier.

Deux autres compétences, un savoir, et un savoir technologique respectivement la connaissance des « Concepts et pratiques d'audit », ainsi que la connaissance de « Environnement général du SI de l'entreprise (environnement d'exploitation de l'ERP, base de données, etc) » n'ont pas été retenus non plus dans le tableau ci dessus. Cette décision s'explique pour les mêmes raisons que pour les savoir-être. Un individu exerçant la fonction d'Auditeur en Sécurité de l'Information ne peut se passer de ces compétences sans quoi son professionnalisme et donc ses pratiques risqueraient d'être remis en cause.

A l'inverse, trois autres compétences, ont été rajoutées suite aux évaluations des experts. Ces trois compétences s'expriment à travers les deux tâches les plus impactées de l'activité 1 « Contextualiser la mission d'audit ». Il s'agit d'un savoir, d'un savoir-faire et d'un savoir technologique :

- Définir l'objectif et le programme d'audit correspondant
- Identifier et prendre en compte des données stratégiques de l'application de normes et de standards
- Intégration de nouvelles technologies au système d'information

Les experts ont souhaité les faire figurer pour insister sur l'importance non seulement de la bonne mise à jour de ses connaissances mais également sur sa capacité à bien cerner le scope de la mission.

Les compétences clés sélectionnées sont donc celles qui ont été considérées par les experts comme essentielles pour se préparer au devenir du métier d'Auditeur en Sécurité de l'Information. Ces compétences seraient ainsi amenées à prendre (encore) davantage d'importance dans la pratique du métier étudié.

3. Les compétences nouvelles pour l'Auditeur 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 d'Auditeur 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 **9 compétences nouvelles** au regard du profil professionnel existant d'Auditeur en Sécurité de l'Information. (Ci après le tableau récapitulatif correspondant à cette réflexion)

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

Aujourd'hui, la pratique des audits se fait 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 différentes évaluations. Cela accentuera les exigences demandées en terme de délais / qualité pour réaliser les Audits en Sécurité de l'Information.

Il y aura également un accroissement (intensification) du besoin de connaissances des systèmes et de certifications internationaux. 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.

Dans le tableau récapitulant les compétences nouvelles du métier d'Auditeur en Sécurité de l'Information, la typologie des compétences nouvelles identifiées illustre dans la même logique que les compétences clés, une dominance des savoir-faire. Ces derniers sont développés dans le tableau.

Contrairement aux compétences clés, deux savoir-être figurent dans l'identification des compétences nouvelles. Ils ont été formulés par les experts pour étoffer le profil relationnel de l'Auditeur en Sécurité de l'Information. Ils ont été exprimés pour faire prendre conscience à ceux qui exercent ce métier des conséquences des exigences qui vont être demandées de plus en plus aux professionnels de ce métier.

Par ailleurs, au niveau des savoirs technologiques, un Auditeur en Sécurité de l'Information devrait davantage pour 2010, faire appel à des connaissances liées aux mécanismes de fonctionnement des systèmes d'information en entreprise pour réaliser ses missions d'audit. A ce titre, il se devra, selon les experts d'accroître ses connaissances dans ce registre pour bien identifier les logiques des flux d'informations qui peuvent être présentes en entreprise.

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

Types de compétences	Éléments nouveaux exprimés	Synthèse des commentaires justificatifs exprimés par les experts
Savoir	Augmenter ses connaissances des lois liées à la protection de la vie privée (données personnelles) dans la sphère professionnelle	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 œuvre 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. 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 politique de Sécurité de l'Information. Ces modifications de pratiques de travail devront s'inscrire au regard des éléments normatifs tel que la norme ISO 27001.
Savoir-faire	Elaborer des outils, des dispositifs de veille pour la mise à jour des connaissances nécessaires à la réalisation des missions d'un Auditeur en Sécurité de l'Information	Cette mise à jour des connaissances orchestrée et systématisée se ferait notamment pour les connaissances nécessaires aux processus de certification appliqués à la Sécurité de l'Information
	Intégrer l'évaluation du risque de sécurisation de l'information en fonction de l'adéquation entre Ressources Humaines et responsabilités/tâches allouées	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
	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	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 dans le cadre du programme d'audit. 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
	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)
Savoir-être	Faire respecter son intégrité dans le déroulement et l'analyse de son travail (que l'auditeur soit en interne ou en externe)	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
	Savoir évoluer dans une logique de co construction entre junior et senior	Le souci du transfert de connaissances entre auditeur senior et junior ou entre auditeur d'un même niveau travaillant sur une même mission est apparu 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
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.

4. Les orientations à investiguer par les organismes de formation

A partir des informations fournies préalablement, un tableau a été créé pour permettre aux acteurs de la formation d'avoir une meilleure visibilité sur ce qui pourrait être nécessaire de proposer en matière de formation à des Auditeurs en Sécurité de l'Information. Plusieurs questions ont permis sa réalisation au regard des tâches qui ont été les plus impactées par le scénario d'évolution du domaine de la Sécurité de l'Information. L'identification des compétences qui en résulte, doit faciliter la constitution ou l'adaptation de modules de formation pour former au mieux des Auditeurs en Sécurité de l'information.

- Quelles sont les compétences considérées comme des **pré-recquis** à l'exercice du métier d'Auditeur en Sécurité de l'information?
- Quelles sont les compétences **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 **spécifiques à une seule activité** du métier d'Auditeur en Sécurité de l'Information ?
- Quelles sont les compétences qui sont **spécifiques à une tâche** et donc à un contexte d'utilisation ?
- Quelles sont les compétences qui sont apparues **critiques** pour la réalisation de multiples tâches de par les résultats des évaluations des experts?
- Quelles sont les compétences clés ré-évaluées?
- A quel **contexte d'utilisation**, est-il possible d'associer les **compétences nouvelles** ?

Ce tableau n'a pas valeur prescriptive. Il cherche avant tout à proposer une aide à la décision pour établir le profil de formation du métier d'Auditeur en Sécurité de l'Information qui soit le plus adéquat aux changements dont le métier en question va devoir faire face à horizon 2010.

Types de questionnements	Types de compétences	Activité(s) / tâches associée(s)	Compétences
Pré-recquis	Savoir être	Quelques soient les activités et tâches identifiées pour le métier étudié	- Analyste - Diplomate - Aisance relationnelle - Curieux - Ouvert d'esprit - Rigoureux - Méthodique
	Savoir Technologique		- Environnement général du Système d'Information
	Savoir		- Concept et pratique d'Audit
Transverse à plusieurs activités	Savoirs		- Normes, méthodes, outils et référentiel qualité sécurité (ITIL, ISO 17799, ISO 27001)
			- Processus business
Spécifique à une seule activité	Savoir-faire	Activité 1	- Se tenir informé des évolutions réglementaires, du référentiel de base, des normes, standards et du contexte de l'entreprise
	Savoir-faire	Activité 2	- Effectuer la collecte des données et l'agrégation des données - Faire un audit de l'architecture réseau, des procédures d'exploitation, du logiciel serveurs, du matériel, du système d'exploitation
	Savoirs		- Normes et procédures de sécurité IT
Spécifiques à une seule tâche	Savoir	Tâche 1.1	- Méthodes de gestion et d'analyse de risques
	Savoir technologique		- Intégration de nouvelles technologies au système d'information
	Savoir-faire	Tâche 1.2	- Définir l'objectif et le programme d'audit correspondant - Identifier et prendre en compte des données stratégiques de l'application de normes et standards

Types de questionnements	Types de compétences	Activité(s) / tâches associée(s)	Compétences
Spécifiques à une seule tâche	Savoir-faire	Tâche 2.1	- Dialoguer – interroger – interviewer des collaborateurs - Elaborer un questionnaire d'audit
	Savoir		- Techniques d'entretien propres à l'audit
	Savoir-faire	Tâche 5.4	- Réaliser des supports d'informations sur le déroulement de l'audit
Critique	Savoir	Tâches 1.1 & 4.4	- Normes professionnelles d'audit
	Savoir-faire	Tâche 1.2 & 2.5	- Analyser de l'information technique et organisationnelle (revue de procédures internes, historiques de l'entreprise)
		Tâche 2.5 & 4.4	- Mettre en place des indicateurs afin de s'assurer de l'application de normes et standards
Contexte d'utilisation pour les compétences nouvelles	Savoir	Activité 1	- Connaissances des lois liées à la protection de la vie privée
	Savoir-faire	Activité 1	- Elaborer des outils, des dispositifs de veille
		Activité 1 & 2	- Identifier les bons interlocuteurs (en matière de compétences, de positionnement dans l'organisation)
			- Evaluer/estimer de manière plus fine le temps adéquat pour la réalisation/le déroulement du programme d'audit et en dresser le programme
	Savoir technologique		- Connaissance, capacité accrue d'identification des flux d'informations liés au fonctionnement d'un système d'information
	Savoir-faire	Activité 2	- Intégrer l'évaluation du risque de sécurisation de l'information en fonction de l'adéquation entre RH et responsabilités/tâches allouées - S'assurer de la cohérence/pertinence du programme d'audit au regard du contexte d'utilisation de ce dernier
Savoir-être	Activité 4	- Savoir évoluer dans une logique de co construction entre junior et senior	
	Transverses à toutes les activités	- Faire respecter son intégrité dans le déroulement et l'analyse de son travail	

A partir de ce tableau, il est donc possible d'appréhender au mieux l'acquisition des compétences clés et nouvelles à l'exercice du métier à horizon 2010. Le cadre de mise en œuvre des 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 ces contenus pédagogiques, quelques questions⁵ repères peuvent permettre aux organismes de formation de déterminer jusqu'où ils souhaitent aller dans l'acquisition de ces compétences.

- La matrice globale dans son état actuel vous paraît-elle suffisamment explicite et exploitable ?
- N'y a-t-il pas des nuances ou des degrés de maîtrise de certaines compétences qu'il serait nécessaire de préciser ?
- Quelles sont les compétences requises auxquelles vous pensez que les organismes de formation doivent pouvoir 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 ?
- Dans les compétences nouvelles recensées : à quelle (autre) activité ou (autre) tâche correspond au sein de votre institution la compétence que vous estimez que les étudiants pourront acquérir lors du cours « Y » ?

⁵ Ces questions sont extraites du guide utilisateur de la démarche d'anticipation des compétences, disponible sur le site www.abilitic.eu



- Au regard des compétences clés et nouvelles qui seront nécessaires à l'horizon 2010 (résultat du projet Abilitic), dans quelle direction votre institution devrait s'orienter en matière de politique pédagogique ?

Conclusion

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

Par ailleurs, lors d'une présentation des résultats auprès de professionnels du domaine de la Sécurité en région lorraine, ces derniers ont fait mention de la nécessité de préparer également l'Auditeur à appréhender davantage les conséquences de son passage au sein d'une organisation. Le déroulement d'un audit engendre en effet un certain nombre de crispations qui si elles ne peuvent être évitées, doivent être réduites autant que possible. Les résultats de l'évaluation et de l'examen des politiques de Sécurité de l'Information sont indéniablement dépendants de la manière dont s'est déroulée la mission d'audit. Cette réflexion doit compléter l'ensemble des éléments qui ont été préalablement présentés.

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 CSO⁶. En effet, un bilan mitigé ressort en matière de mise en place et de surveillance des politiques de sécurité au niveau international, Luxembourg compris. En effet, 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 l'Auditeur en Sécurité de l'Information peut apporter une expertise dans l'évaluation et l'examen des politiques liées à la sécurité et à la confidentialité des informations transmises. La focalisation que les experts ayant participé à la démarche d'anticipation, ont fait notamment sur les activités de contextualisation et de déroulement de la mission d'audit doit permettre de répondre au mieux aux problématiques relevées précédemment.

Les résultats de l'étude doivent donc être appréhendés comme des pistes sérieuses, partagées par un collectif d'experts et devant faciliter l'adaptation des programmes de formation qui préparent à l'exercice de la fonction d'Auditeur en Sécurité de l'Information.

⁶ L'étude intitulée "Global State of Information Security Survey 2007" est disponible sur le site 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"