Document ENISA:

Plaquette d'information pour les PME

comportant des exemples
d'évaluation et de gestion des risques
portant sur deux PME

(également disponible à l'adresse www.enisa.europa.eu/rmra)

Réalisée par le
département technique de l'ENISA
section Gestion des risques
en coopération avec:

M. George Patsis
Obrela Security Industries (OSI)
www.obrela.com

Février 2007

Avis juridique

Résumé

Le présent document correspond au second résultat prévu dans le programme de travail 2006 de l'ENISA. Il est en partie basé sur la nécessité communiquée à l'ENISA d'une approche d'évaluation des risques simplifiée.

Le présent document a pour objet de fournir une présentation complète et simplifiée de l'évaluation/gestion des risques à l'usage des petites et moyennes entreprises (PME). À cet effet, le présent document a été structuré en modules. Il est constitué de différentes parties qui sont respectivement consacrées aux besoins spécifiques des parties prenantes impliquées dans le processus d'évaluation des risques et de gestion des risques.

L'idée sous-jacente à l'élaboration de ce document a été de soutenir les utilisateurs (non experts) face à la complexité des activités de gestion des risques et d'évaluation des risques. Certaines questions complexes de sécurité ont ainsi été simplifiées et limitées au minimum nécessaire pour assurer un niveau de sécurité acceptable.

Dans les cas où un niveau de sécurité élevé est exigé, il faudra sans aucun doute considérer la gestion de la sécurité dans sa totale complexité et s'immerger dans le contenu détaillé des mesures et technologies correspondantes. À cet égard, les idées et l'approche présentées ici sont censées couvrir un niveau de sécurité acceptable pour les petites organisations comportant des investissements modestes en matière de sécurité. Des formes plus évoluées de sécurité (par exemple, les éléments d'une infrastructure critique) exigeraient un traitement plus approfondi qui dépasse le cadre du présent document.

Ce document a été élaboré en anticipant l'ensemble des compétences des différentes parties prenantes impliquées dans l'évaluation des risques. Le processus proposé d'évaluation des risques est structuré à l'aide d'une approche d'évaluation simplifiée en quatre phases. Nous supposons que les utilisateurs de ce document n'ont pas de connaissances avancées sur les questions de sécurité. Si de telles connaissances s'avèrent nécessaires, l'approche utilisée est de représenter une «boîte noire» offrant un nombre limité de choix complets.

Un autre critère pris en compte a été la rentabilité à tous les stades de l'évaluation des risques et de la gestion des risques. Le présent document peut aider les décideurs à choisir quelle approche d'évaluation des risques est la plus appropriée pour leur organisation, en se basant sur les indicateurs de coûts et de performances. En outre, dans le cas où l'auto-évaluation a été choisie, ce document fournit les outils nécessaires pour l'effectuer, sans exiger une précédente expérience dans ce domaine.

L'approche simplifiée d'évaluation des risques présentée dans ce document est un exemple de bonnes pratiques pour évaluer les risques liés à l'information. On suppose qu'il existe d'autres approches/bonnes pratiques similaires qui pourraient être utilisées à sa place. Ainsi, la présente approche ne vise ni à remplacer des normes existantes ni à redéfinir les bonnes pratiques. Elle est plutôt destinée à fournir aux PME intéressées un outil qu'elles ne pourraient pas trouver aisément ailleurs.

La mise en pratique des idées présentées ici a été démontrée à l'aide d'exemples. Deux types représentatifs de PME ont été choisis dont les risques sont évalués à l'aide de la présente approche d'évaluation. Ces exemples sont présentés dans le cadre de l'approche simplifiée d'évaluation des risques.

Il convient de mentionner que ce document est le premier d'une série de documents qui seront publiés par l'ENISA pour sensibiliser les PME à l'évaluation des risques et à leur gestion. Le document, dans sa version actuelle, est appelé à subir d'éventuelles améliorations, adaptations et expansions. Les activités de l'ENISA comprendront à l'avenir la validation de ce document dans le cadre de projets pilotes menés au sein des PME, l'évaluation/la révision par des équipes d'experts, la diffusion par des associations professionnelles et/ou de formation, etc. L'objectif final est de disposer d'une version de ce document utilisable «en l'état» par les PME, c'est-à-dire qui ne requiert pas d'autre amélioration, explication ou adaptation. En attendant, nous faisons donc référence au présent document en le qualifiant de «version bêta» ce qui signifie que des améliorations et des ajustements seront apportés après plusieurs expériences pilotes, déploiements et diffusions qui permettront, à moyen terme, au document présenté de mûrir.

Données de contact: département technique de l'ENISA, section Gestion des risques, Dr. L. Marinos, expert responsable de la gestion des risques, adresse électronique: RiskMngt@enisa.europa.eu

Sommaire

Figures

Tableaux

1. Objet et champ d'application

Les petites et moyennes entreprises (PME) constituent un domaine prioritaire pour la politique économique gouvernementale et leur importance est considérée comme primordiale pour la croissance socio-économique au sein de l'Union européenne. Généralement créées grâce à la passion entrepreneuriale de leur fondateur et avec des financements limités, les PME ont des systèmes internes souvent hétérogènes et indépendants. En outre, les actifs corporels et incorporels des PME sont définis de façon approximative, et la valeur de ces actifs n'est souvent que partiellement connue. C'est typiquement le cas en ce qui concerne l'un des actifs les plus importants, à savoir, l'information.

À l'instar des autres actifs de l'entreprise, l'information doit être stratégiquement gérée et protégée. Assurer la sécurité de l'information dans une entreprise consiste à protéger l'information ainsi que les systèmes et le matériel utilisés pour stocker, traiter et transmettre l'information. Les chefs d'entreprise doivent impérativement prendre conscience de la valeur de l'information contenue dans leurs systèmes internes et doivent prévoir un cadre d'évaluation et de mise en œuvre de la sécurité de l'information. De nombreux cadres et programmes de sécurité approuvés à l'échelle internationale peuvent être mis en place pour protéger une organisation contre la perte d'information et le risque de voir sa responsabilité engagée. Mais ces cadres souvent complexes, englobant une multitude de fonctionnalités et coûteux à mettre en œuvre, sont généralement plus adaptés pour les grandes entreprises.

Habituellement, en raison du mode de développement des PME, dynamique et adapté aux circonstances, ces dernières ne prévoient jamais systématiquement les questions de sécurité et d'intégration lors de la phase de création. Ainsi, les politiques de planification de la sécurité de l'information et plans anti-sinistre sont-ils souvent très rudimentaires, voire même inexistants. Il est courant que les connaissances de base des PME en matière de risques liés à la sécurité de l'information se limitent à l'existence des virus et des logiciels antivirus. Les menaces accidentelles représentent des risques importants pour la sécurité de l'information des PME et pourtant les programmes de sensibilisation et de formation du personnel dans ce domaine sont souvent négligés.

Les résultats d'une enquête révèlent que le niveau de sensibilisation à la sécurité de l'information parmi les chefs d'entreprise est aussi variable que l'état de leurs systèmes d'information, et de leur technologie et sécurité de l'information. Bien qu'un petit nombre de PME adopte des cadres de sécurité tels que celui de la norme ISO/IEC 27001 ou de la norme internationale ISO 17799, la plupart des responsables de PME n'ont pas entendu parler des normes sur la sécurité et pensent que la sécurité de l'information se résume à une intervention technique destinée à faire face aux menaces de virus et à la sauvegarde des données.

Sans reprocher aux responsables de PME d'ignorer l'importance de la sécurité de l'information, l'enquête conclut que les dirigeants d'entreprise doivent comprendre, engager et mettre en œuvre des processus formels de sécurité de l'information, ainsi que des mesures techniques et organisationnelles. Faute de quoi, leurs organisations risquent d'être gravement affectées par des menaces accidentelles ou des attaques délibérées à l'encontre de leurs systèmes d'information qui pourraient au final entraîner la faillite de leur entreprise.

En s'appuyant sur le contenu de cette plaquette d'information, les PME pourront effectuer une évaluation des risques de leur environnement, sélectionner et appliquer des mesures adaptées pour gérer les risques liés à la sécurité de l'information. Dans ce document, nous aidons les PME à définir de tels efforts dans ce domaine, à décider de la façon de les déployer et, si elles ont suffisamment de ressources, nous leur donnons des conseils pour effectuer une auto-évaluation des risques liés à l'information. À cet effet, nous proposons une méthode simple d'évaluation des risques qui permet une identification rapide et complète des risques liés à l'information, et leur réduction.

La méthode d'évaluation présentée dans ce document est basée sur un modèle simplifié qui a été élaboré pour de petites organisations ayant certaines caractéristiques en commun. Premièrement, leur structure organisationnelle est relativement linéaire, et les personnes des différents niveaux

organisationnels sont habituées à travailler ensemble. Deuxièmement, les membres du personnel doivent souvent effectuer un grand nombre de tâches, et ont donc affaire à divers processus et procédures utilisés dans l'ensemble de l'organisation.

2. Structure du document

Nous avons choisi d'adopter une structure modulaire pour ce document afin de couvrir les besoins des divers types de PME. Les différentes parties du document pourront s'avérer utiles en fonction des besoins d'une PME donnée et de sa détermination à effectuer une évaluation des risques. Pour les PME qui ont besoin d'avoir un aperçu de la gestion des risques dans le but de définir leur stratégie d'avenir, la partie générale du présent document sera utile (voir chapitre 3. Recommandations pour le décideur et chapitre 4. Une approche simplifiée: présentation).

Si une PME décide de mettre en œuvre sa propre gestion des risques, il est impératif qu'elle lise les parties de ce document comprenant la description détaillée de la méthode de gestion des risques et les exemples (voir chapitre 5. Conseils pour l'auto-évaluation avec deux exemples). En cas d'auto-évaluation, le contenu détaillé des annexes sera nécessaire pour définir les mesures à mettre en œuvre au sein de l'organisation (voir Annexe A. Cartes de contrôles organisationnels, Annexe B. Cartes de contrôles des actifs). Pour faciliter l'utilisation de cet ouvrage, nous donnons quelques exemples basés sur différentes finalités des lecteurs potentiels:

- **Personnes avec une expérience de la direction**: le chapitre 3 sur les décideurs est recommandé. Il explique le contexte de la sécurité de l'information et la nécessité de gérer les risques. Il esquisse les options possibles pour mettre en œuvre la gestion des risques et définit les critères de décision. Les dirigeants intéressés auront peut-être envie de comprendre la structure du processus d'évaluation des risques proposé dans ce document, telle que présentée au chapitre 4.
- **Membres sans expérience d'une équipe d'évaluation des risques**: les membres d'une équipe d'évaluation des risques auront besoin de comprendre l'approche simplifiée d'évaluation des risques qui est proposée, de lire sa description détaillée ainsi que les exemples présentés (voir chapitre 4. Une approche simplifiée: présentation).
- **Membres experts d'une équipe d'évaluation des risques**: les membres experts d'une équipe d'évaluation des risques devront lire la méthode et comprendre les détails. Ils seront également en mesure de consulter les données présentées dans les annexes, notamment concernant le choix des mesures (également citées en tant que contre-mesures, contrôles ou contrôles de sécurité dans ce document). De nouvelles mesures peuvent être affectées pour les actifs existants ou de nouveaux actifs peuvent être rajoutés (voir Annexe A. Cartes de contrôles organisationnels, Annexe B. Cartes de contrôles des actifs et Annexe C. Contrôles organisationnels).

3. Recommandations pour le décideur

3.1 Aspects à prendre en considération

Aujourd'hui, les informations créées, traitées et utilisées par une organisation comptent parmi ses actifs qui ont le plus de valeur. La divulgation, compromission ou indisponibilité de cet actif peut avoir un **grave impact** sur une organisation, constituer un **délit de droit commun ou violation des règles**, et nuire à son **image**.

Assurer la sécurité adéquate de l'information et des systèmes de traitement de l'information compte parmi les principales responsabilités de la direction. Les propriétaires et décideurs doivent bien comprendre l'état actuel de leur programme de sécurité de l'information pour pouvoir prendre des décisions bien fondées et faire des investissements pertinents qui limitent les risques à un niveau acceptable. Transposés à des activités vitales ou à des aspects juridiques de l'entreprise, les risques liés à l'information pourraient conduire à des situations critiques. On peut notamment citer les catégories de risques critiques suivantes:

- **Risques juridiques / de conformité:** il s'agit des risques découlant de violations ou de non respect de lois, règles comptables, pratiques recommandées, ou normes éthiques. Les risques juridiques ou de conformité peuvent exposer une organisation à une publicité négative, des amendes, des sanctions pénales et des sanctions financières civiles, au paiement de dommages et intérêts, et à l'annulation de contrats. Le vol d'informations sur un client telles que les informations relatives à la carte de crédit, les informations financières, les informations relatives à la santé, ou les données personnelles risque de donner lieu à des réclamations de tierces parties. **Conscients que la sécurité de l'information est un problème de plus en plus important aux multiples facettes, et dans le souci de protéger les droits des citoyens et d'assurer la responsabilité des entreprises, les gouvernements de l'UE et l'Union européenne ont instauré des lois et règlements qui exigent la mise en conformité des organisations, indépendamment de leur taille ou du domaine industriel. Ces règlementations imposent aux entreprises de mettre en œuvre des contrôles internes visant à les protéger contre les risques liés à l'information. Elles visent aussi à améliorer les pratiques et procédures de gestion des risques.**
- **Risques liés à la stabilité financière:** faute d'infrastructures de production et de gestion appropriées et faute de personnel capable de mettre en œuvre la stratégie de l'entreprise, celle-ci peut échouer à atteindre les buts fixés et les objectifs financiers énoncés. La **gestion inadéquate de la sécurité de l'information peut entraîner des risques liés à la stabilité financière de l'organisation. De tels risques, à leur tour, peuvent ouvrir la voie à des problèmes de fraude, blanchiment d'argent, instabilité financière, etc**.
- **Risques liés à la productivité:** il s'agit de risques de pertes opérationnelles et **prestations de services médiocres aux clients** qui découleraient du manque d'adhésion aux procédures et contrôles fondamentaux de traitement. Cela fait généralement référence à toutes les activités coopératives de production, qui contribuent d'une certaine manière à la fourniture globale d'un produit ou d'un service. Les risques liés à la productivité ne sont pas limités à l'utilisation de la technologie; ils peuvent aussi résulter d'activités organisationnelles. Le risque découlant de systèmes ou d'applications logicielles mal ou insuffisamment contrôlés, utilisés en première ligne, des opérations de gestion des risques, de la comptabilité ou d'autres unités, est classé dans cette famille de risques. La gestion inadéquate de la sécurité de l'information peut exposer l'entreprise à des risques importants liés à la productivité, notamment des coûts d'exploitation élevés, des déficiences opérationnelles, de mauvaises décisions de gestion (prix, liquidité, et exposition au risque de crédit frauduleux), et le manque **de confidentialité et l'interruption du service aux clients**.

- **Renommée et confiance des clients:** le risque le plus difficile à comprendre, mais néanmoins le plus important, est peut-être le risque que la renommée de l'organisation soit compromise; la renommée étant un actif intangible mais de grande valeur. Les clients indiqueront-ils leur numéro de carte de crédit à une entreprise, une fois qu'ils auront lu dans le journal qu'elle a été piratée? Les cadres resteront-ils dans une société confrontée à un tel problème? Et, quelle sera la réaction des actionnaires de l'entreprise? Quelle sera la perte prévue de revenu? Quelle sera la perte prévue de marchés potentiels?

De nombreux propriétaires de PME pensent qu'ils ne sont pas exposés à de tels risques en raison de la taille réduite de leur entreprise et de l'actif informationnel. La plupart d'entre eux pense que les grandes entreprises avec un plus grand volume d'information sont les seules exposées à de tels risques. Ce n'est pas vrai. Premièrement, la sensibilité de l'information dépend de la nature et non de la quantité d'information. Deuxièmement, les PME n'ont pas autant de ressources ni autant de personnel disponibles que les grosses entreprises pour régler les problèmes de sécurité, de sorte qu'elles sont plus exposées. En effet, les nouvelles technologies permettent aux petites entreprises d'utiliser les mêmes systèmes d'information que ceux employés par les grandes entreprises. Les petites entreprises qui les utilisent, s'exposent donc aux nombreux risques qui étaient traditionnellement associés aux grandes organisations. **De fait, 56 pour cent des petites entreprises ont connu au moins un incident de sécurité au cours de l'année passée**. Malheureusement, parmi les entreprises confrontées à une défaillance informatique majeure, nombreuses sont celles qui ne s'en remettent pas et qui font faillite. Il est donc impératif que les propriétaires et responsables de PME identifient ces pièges et prennent des mesures pour prévenir les problèmes de sécurité de l'information.

Les mesures de réduction des risques liés à la sécurité de l'information (contrôles) devraient être proportionnelles aux risques existants pour l'information en question. Mais le processus qui consiste à déterminer quels sont les contrôles de sécurité appropriés et rentables, est souvent assez complexe et peut parfois s'avérer subjectif. **L'évaluation permanente des risques liés à la sécurité est l'une des principales fonctions qui permettent d'établir ce processus sur une base plus objective**.

3.2 Connaissances indispensables

La sécurité de l'information consiste à identifier, réduire et gérer les risques importants pour les actifs informationnels. L'évaluation des risques est la première phase nécessaire pour comprendre les risques en effectuant une **identification** et une **estimation** complètes des risques liés à la sécurité d'une organisation. Les résultats d'une telle activité sont essentiels pour gérer l'entreprise dans la mesure où les risques impliqués peuvent influencer de manière significative la confidentialité, l'intégrité et la disponibilité des actifs informationnels et **s'avérer essentiels pour le maintien de l'avantage concurrentiel, la stabilité financière, la conformité juridique et la préservation d'une image commerciale forte**.

L'évaluation des risques peut aider les décideurs à:

- **évaluer les pratiques organisationnelles et la base de la technologie installée;**
- **imposer une protection de l'information basée sur l'impact potentiel sur l'organisation;**
- **centrer les activités de sécurité sur les aspects importants. Les mesures qui sont associées à des risques acceptables peuvent être abandonnées;**
- **veiller à ce que les mesures et les dépenses engagées soient proportionnelles aux risques auxquels l'organisation est exposée. Il s'agit ainsi de trouver l'équilibre entre les coûts associés au traitement d'un risque et les bénéfices tirés de la prévention de son impact négatif.**

Lors de l'évaluation des risques, une organisation effectue des activités destinées à (a) identifier les risques liés à la sécurité de l'information, (b) évaluer les risques pour déterminer les priorités et (c) définir des mesures de réduction des risques (voir aussi Figure 1).

L'évaluation des risques liés à la sécurité de l'information n'est pourtant que la première étape vers la gestion des risques liés à la sécurité de l'information, qui est définie comme le processus continu d'identification des risques et de mise en œuvre de plans visant à y faire face. La figure 1 illustre un processus de gestion des risques liés à la sécurité de l'information et le «sous-ensemble» que constitue l'évaluation des risques.

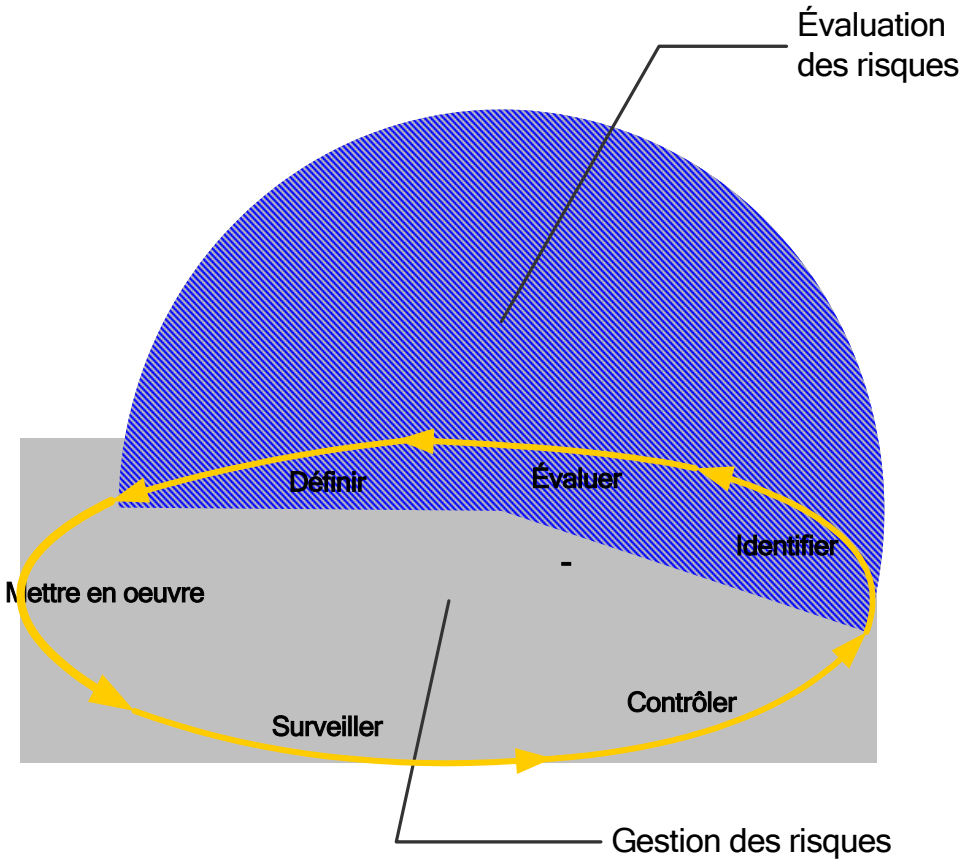

Figure 1: Activités d'évaluation des risques par rapport à la gestion des risques liés à la sécurité de l'information

De toute évidence, l'évaluation des risques à proprement parler permet à une organisation d'orienter ses activités en matière de sécurité de l'information; elle **ne conduit pas nécessairement à une amélioration importante sauf si des mesures ont été mises en œuvre**. Comme dans toute autre discipline de gestion, la mise en œuvre d'une partie du cycle de gestion ne suffit pas à elle seule à produire les effets désirés. Aucune évaluation, quels que soient son degré de détail et son niveau d'expertise, n'améliorera la situation de la sécurité à moins que l'organisation ne poursuive ses efforts jusqu'à la mise en œuvre. Outre l'évaluation des risques, la gestion réelle des risques inclut les **étapes suivantes**:

- **Planifier** la manière de mettre en œuvre la stratégie de protection et les plans de réduction des risques à partir de l'évaluation en développant des plans d'action détaillés. Cette activité peut englober une analyse coûts/bénéfices détaillée des différentes stratégies et actions.
- **Mettre en œuvre** les plans d'action détaillés retenus.

- **Surveiller** l'avancement et l'efficacité des plans. Cette activité implique de surveiller tout éventuel changement dans les niveaux de risque.
- **Contrôler** les variations dans l'exécution du plan en prenant des actions correctives appropriées.

3.3 Approches en matière de sécurité de l'information

Entre autres responsabilités, il incombe aux dirigeants de PME d'assurer la sécurité de l'environnement de leur entreprise. Selon la plupart des dispositions légales applicables, ils sont seuls responsables en cas de manquement aux règles de sécurité. Ils doivent non seulement s'assurer que l'environnement physique est sûr et sécurisé, mais également veiller à la protection de l'information. De fait, la sécurité des ordinateurs n'étant pas garantie à tout jamais, il faut toujours se soucier de la protection de l'information.

Les décideurs peuvent entreprendre une évaluation des risques de leur environnement et introduire des mesures adéquates pour faire face aux risques inacceptables. C'est la condition préalable à la gestion de la sécurité de l'information. Différentes approches sont disponibles pour l'affectation des effectifs à cet effort (on parle également de décision de type «faire ou faire faire»). Nous faisons la distinction entre les trois approches suivantes:

- **Internalisation de l'évaluation des risques**: l'évaluation des risques et l'identification des mesures nécessaires sont effectuées par le personnel interne. L'évaluation est basée sur une approche d'évaluation des risques sélectionnée par l'organisation (par exemple, les bonnes pratiques, une norme connue, etc.). Cela aidera l'organisation à maîtriser cette approche dans la perspective d'une exécution récurrente.
- **Externalisation totale de l'évaluation des risques**: suivant cette approche, l'évaluation complète des risques est réalisée par un contractant extérieur. L'évaluation est basée sur une approche d'évaluation des risques qui est choisie par le contractant extérieur. Le contractant peut aussi se charger des futures évaluations récurrentes. Aucun transfert de savoir-faire au personnel interne n'est prévu pendant toute la durée du cycle de l'évaluation/gestion des risques de la PME.
- **Externalisation partielle de l'évaluation des risques**: cette approche suppose que l'évaluation initiale des risques est effectuée par une société extérieure. L'évaluation sera basée sur une approche d'évaluation des risques qui est connue de la PME. D'autres évaluations des risques peuvent donc être effectuées par le personnel interne. L'évaluation initiale effectuée par la société extérieure sert de transfert de savoir-faire au personnel interne de la PME.

Le présent document offre aux PME tout le matériel nécessaire pour décider entre les trois approches précitées. En outre, nous fournissons toutes les informations requises pour aider les PME à effectuer une auto-évaluation. Dans les approches d'internalisation et d'externalisation partielle, l'approche d'évaluation des risques proposée peut servir d'orientation pour l'évaluation initiale des risques et les évaluations à venir (voir chapitres 4. Une approche simplifiée: présentation et 5. Conseils pour l'auto-évaluation avec deux exemples).

Par rapport aux autres approches, chaque approche d'évaluation des risques est associée à des avantages et des inconvénients. Le Tableau 1 offre un aperçu des implications liées à la décision de sous-traiter l'effort d'évaluation ou de l'accomplir en interne. Les paragraphes ci-après contiennent une discussion détaillée sur les paramètres et les facteurs qui devraient être pris en considération par une PME lorsqu'elle sélectionne une approche de gestion des risques.

Options pour la mise en œuvre d'une évaluation des risques	Paramètres et facteurs relatifs à la mise en œuvre				
	Expertise interne requise	Dépendance à l'égard d'une tierce partie	Ressources internes requises	Objectivité de l'évaluation	Effort d'une tierce partie[1]
Internalisation	Oui	Faible	1-5 personnes	Faible	-
Externalisation totale	Non	Élevée	1 Personne (pour la gestion du projet)	Élevée	10-40 jours
Externalisation partielle	Oui	Faible	1-2 personnes	Moyenne	5-10 jours

Tableau 1: Options pour la mise en œuvre de l'évaluation des risques

Dans les paragraphes suivants, nous décrivons chaque option possible pour procéder à l'évaluation/gestion des risques. Un questionnaire aidera les décideurs à déterminer si cette option est appropriée pour un type donné de PME.

3.3.1 Internalisation

L'internalisation peut offrir de nombreux **avantages tels que le développement du savoir-faire et de la compétence de l'organisation en matière d'évaluation des risques et de gestion des risques. De surcroît, selon les prix des services de conseil en matière de sécurité, cette approche peut permettre une réduction des dépenses.** C'est une option particulièrement attractive pour les organisations ayant une structure simple, qui ont une expérience réussie dans la mise en œuvre en interne d'activités similaires (par exemple, norme ISO9001), et dotées des capacités et compétences adéquates.

La série de questions suivante peut aider à déterminer si la réalisation de l'évaluation des risques en interne est la bonne décision pour une organisation:

Questions pour la prise de décision	Réponse	
	☺ Oui	☹ Non
Votre organisation est-elle de petite taille? A-t-elle une structure hiérarchique linéaire ou simple?		
Avez-vous un **savoir-faire interne en matière de systèmes TI et de réseaux?**		
Votre organisation a-t-elle des ressources humaines qualifiées et disponibles?		
Les activités de votre entreprise sont-elles relativement peu		

[1] Nous supposons une PME avec des effectifs allant jusqu'à 100 personnes.

dépendantes des systèmes TI et sans lien avec le stockage ou le traitement des données clients sensibles; votre organisation a-elle été impliquée dans des activités similaires, par exemple, dans des processus d'amélioration de la qualité?		
Pouvez-vous trouver trois à cinq personnes ayant une connaissance approfondie et complète de l'organisation et qui auraient la plupart des compétences suivantes? ▫ aptitude à résoudre les problèmes ▫ compétences analytiques ▫ esprit d'équipe ▫ qualités d'encadrement ▫ **aptitude à comprendre les processus internes de l'entreprise et l'infrastructure sous-jacente de l'organisation** ▫ possibilité de consacrer quelques jours à travailler sur cette méthode		
L'infrastructure de technologie de l'information de votre entreprise est-elle relativement simple et bien comprise par au moins une personne dans votre organisation?		

Plus il y a de réponses affirmatives, plus l'auto-évaluation est susceptible d'être le bon choix pour une PME.

À l'aide de l'approche proposée d'évaluation des risques et des meilleures pratiques (voir chapitres 4. Une approche simplifiée: présentation et 5. Conseils pour l'auto-évaluation avec deux exemples) les décideurs seront en mesure d'entreprendre des évaluations des risques en adoptant une approche efficace d'identification et de gestion des risques liés à la sécurité de l'information, ce qui leur permettra d'améliorer constamment la situation de la sécurité au sein de leur organisation.

3.3.2 Externalisation totale

Dans le cadre d'une externalisation totale, une PME confie l'ensemble de l'évaluation des risques et de la gestion des risques à un contractant extérieur. Cette démarche peut inclure les activités initiales et récurrentes d'évaluation et de gestion qui couvriront l'ensemble du cycle de gestion des risques (par exemple, mise en œuvre et entretien des mesures). Le contractant applique sa propre approche d'évaluation/gestion des risques. Ainsi, il n'y a aucun transfert de savoir-faire au client. À ce stade, il convient de noter que l'externalisation des activités d'évaluation et de gestion ne dégage pas la direction de la PME de sa responsabilité en matière de sécurité (de l'information).

En fonction de la structure, de la stratégie, des ressources disponibles et de la situation du marché, l'externalisation **peut offrir des avantages manifestes**. La décision d'externaliser l'évaluation des risques liés à l'information permet à la PME de se concentrer sur les principales stratégies commerciales, tout en laissant à un expert extérieur en sécurité de l'information le soin d'effectuer les activités périphériques.

Les questions suivantes peuvent aider à déterminer si la décision d'externaliser la totalité de l'évaluation des risques est appropriée pour une organisation:

Questions pour la prise de décision	Réponse ☺ Oui	Réponse ☹ Non
Jugez-vous nécessaire **d'accorder une attention croissante** aux compétences clés et aux processus internes stratégiques?		
Auriez-vous des **difficultés à trouver deux à cinq personnes** ayant une connaissance approfondie et complète de l'organisation et qui auraient la plupart des compétences suivantes? ▫ **aptitude à comprendre les processus internes de l'entreprise et l'infrastructure sous-jacente de l'organisation** o aptitude à résoudre les problèmes o compétences analytiques o esprit d'équipe o qualités d'encadrement o possibilité de consacrer quelques jours à travailler sur cette méthode		
Avez-vous une **infrastructure TI très complexe et relativement importante**?		
Votre entreprise et votre offre de services comprennent-elles **des transactions financière**?		
Gérez-vous une entreprise qui est soumise à des contraintes et/ou mandats juridiques ou réglementaires stricts, au niveau national ou de l'UE?		
L'infrastructure de technologie de l'information de votre entreprise est-elle relativement simple et bien comprise par au moins une personne dans votre organisation?		

À nouveau, plus il y a de réponses affirmatives, plus l'externalisation est susceptible de satisfaire les besoins de la PME.

Confier les activités d'évaluation des risques à une tierce partie exige un **processus de sélection du fournisseur englobant une vérification au préalable et une estimation globale du fournisseur, ainsi que l'évaluation de la compétence du fournisseur en matière de sécurité de l'information (voir aussi** Annexe E. Conseils simples, Tiers, Prestataires de services**).**

Un accord de niveau de service, le cas échéant, devrait constituer la principale base de coopération et définir les éléments clés tels que la certification professionnelle des ingénieurs de sécurité du fournisseur, ainsi que d'autres aspects relatifs au fournisseur tels que la politique de confidentialité et de non divulgation, le calendrier, l'affectation des ressources, les coûts et la méthodologie employée.

En cas d'accord de niveau service, les questions suivantes devraient être prises en considération (équivalant à une sorte de liste de contrôle sur le contenu de l'accord):

- **Les questions de responsabilité sont-elles couvertes?** Que se produira-t-il, par exemple, si lors de l'évaluation, les principales activités de l'entreprise sont arrêtées ou perturbées en raison de l'incompétence du fournisseur à effectuer une évaluation de l'infrastructure TI et des réseaux sous-jacents?
- **Les responsabilités sont-elles clairement identifiées** par l'accord de niveau de service? Qui sera responsable et de quelles activités? Quelle est l'implication de l'organisation en termes de ressources?

- **Les travaux à effectuer sont-ils clairement établis par écrit**? Qu'est-ce que le fournisseur inclut dans les travaux à effectuer? Il est fortement recommandé que les travaux à effectuer couvrent l'éventail complet des activités de l'entreprise et l'infrastructure sous-jacente. Sinon, le résultat risque d'être inapproprié ou même trompeur.
- **Comment les exigences légales vont-elles être satisfaites,** par exemple, la législation sur la protection des données?
- Quelles dispositions seront prises pour permettre que toutes les parties impliquées dans l'externalisation, y compris les sous-traitants, soient conscients de leurs responsabilités en matière de sécurité?
- Comment l'**intégrité et la confidentialité des actifs de l'organisation vont-elles être assurées et testées?**
- **Quels seront les contrôles physiques et logiques utilisés pour restreindre l'accès aux informations internes sensibles de l'organisation et le limiter aux utilisateurs autorisés?**
- **Comment la disponibilité des services va-t-elle être maintenue en cas de catastrophe?**
- **Le droit d'auditer les mesures de protection de l'information et de sécurité du fournisseur est-il inclus dans les termes et conditions**?
- Les **ressources minimales, les compétences et la certification professionnelle du fournisseur** sont-elles clairement indiquées?
- Les modalités de compte rendu (contenu, fréquence et structure) sont-elles clairement définies?

Les organisations peuvent imposer aux fournisseurs d'effectuer une évaluation basée sur la méthodologie de gestion des risques proposée ici (voir chapitre 5. Conseils pour l'auto-évaluation avec deux exemples). À condition que la PME comprenne le contenu de l'approche proposée, elle sera ainsi en mesure de mieux contrôler les activités du contractant.

3.3.3 Externalisation partielle

Une solution mixte **consiste à combiner les avantages de l'internalisation et de l'externalisation**. Dans le cadre de cette troisième solution, l'organisation participe activement au processus d'auto-évaluation en ayant recours à une tierce partie en qualité d'animateur-formateur. De plus, l'évaluation est basée sur un modèle d'évaluation des risques qui est compris par le client, par exemple l'approche d'évaluation des risques présentée ici (voir chapitre 4. Une approche simplifiée: présentation). Il s'agit là d'une **condition préalable nécessaire pour réaliser un transfert de savoir-faire** entre le contractant et le client.

Dans ce scénario, la PME développe les capacités internes nécessaires pour exécuter les tâches importantes de sécurité, le cas échéant. L'organisation peut ajuster et gérer les coûts du contractant à l'avenir et contribuer significativement à l'expertise fournie par un tiers, expert en la matière, ce qui lui procure des avantages manifestes.

La série de questions suivantes peut aider à déterminer si l'évaluation des risques devrait être partiellement externalisée:

Questions pour la prise de décision	Réponse ☺ Oui	☹ Non
Jugez-vous nécessaire d'accorder une attention croissante aux compétences clés et aux processus internes stratégiques mais également d'améliorer la sensibilisation à la sécurité de l'information en interne et les compétences en matière de sécurité de l'information?		
Pensez-vous pouvoir trouver une ou deux personnes disponibles dans votre organisation, ayant une connaissance approfondie et complète de l'organisation et qui auraient la plupart des compétences suivantes? ▫ **aptitude à comprendre les processus internes de l'entreprise et l'infrastructure sous-jacente de l'organisation** ▫ aptitude à résoudre les problèmes ▫ compétences analytiques ▫ esprit d'équipe ▫ qualités d'encadrement ▫ possibilité de consacrer quelques jours à travailler sur cette méthode ▫ disponibilité à plus long terme		
Avez-vous une infrastructure TI complexe et relativement importante mais un modèle d'entreprise relativement simple?		
Votre entreprise et votre offre de services comprennent-elles des transactions financières?		
Gérez-vous une entreprise qui est soumise à des contraintes et/ou mandats juridiques ou réglementaires stricts au niveau national ou de l'UE?		

Comme pour les précédentes approches, plus il y a de réponses affirmatives, plus cette approche d'évaluation des risques est susceptible d'être le bon choix pour une PME.

L'externalisation partielle de l'évaluation des risques exige un accord de niveau de service comme base principale de coopération avec le contractant. Les éléments clés d'un accord de niveau de service sont la certification professionnelle des ingénieurs de sécurité du fournisseur, la confidentialité, le calendrier, l'affectation des ressources, les coûts et la méthodologie employée. Ici aussi, les organisations peuvent ordonner aux fournisseurs d'effectuer une évaluation basée sur la méthodologie de l'ENISA proposée ici (voir chapitre 4. Une approche simplifiée: présentation).

Les questions suivantes devraient au moins être prises en compte dans le cadre d'un accord de niveau de service conclu pour l'externalisation partielle de l'évaluation des risques liés à la sécurité de l'information:

- Le contractant est-il d'accord pour utiliser une approche d'évaluation des risques prédéfinie qui est également connue du client (par exemple, l'approche d'évaluation des risques proposée ici)?
- **Les questions de responsabilités** sont-elles couvertes? Que se produira-t-il, par exemple, si lors de l'évaluation, les principales activités de l'entreprise sont arrêtées ou perturbées en

raison de l'incompétence du fournisseur à effectuer une évaluation de l'infrastructure TI et des réseaux sous-jacents?

- **Les responsabilités** sont-elles clairement identifiées par l'accord de niveau de service**?** Qui sera responsable de telles ou telles activités? Quelle est l'implication de l'organisation en termes de ressources?
- **Les travaux à effectuer** sont-ils clairement établis par écrit? Qu'est-ce que le fournisseur inclut dans les travaux à effectuer? Il est fortement recommandé que les travaux à effectuer couvrent l'éventail complet des activités de l'entreprise et l'infrastructure sous-jacente. Sinon, le résultat risque d'être inapproprié ou même trompeur.
- Comment **les exigences légales** vont-elles être satisfaites, par exemple, la législation sur la protection des données?
- Quelles dispositions seront prises pour permettre que toutes les parties impliquées dans l'externalisation, y compris les sous-traitants, soient conscientes de leurs responsabilités en matière de sécurité?
- Comment l'**intégrité et la confidentialité des actifs de l'organisation** vont-ils être assurés et testés?
- Quels **contrôles physiques et logiques** seront utilisés pour restreindre l'accès aux informations internes sensibles de l'organisation et le limiter aux utilisateurs autorisés?
- Comment la **disponibilité des services va-t-elle être maintenue en cas de catastrophe?**
- Le **droit d'auditer** les mesures de protection de l'information et de sécurité du fournisseur est-il inclus dans les termes et conditions?
- Les **ressources minimales, les compétences et la certification professionnelle du fournisseur** sont-elles clairement indiquées?
- Les modalités de compte rendu (contenu, fréquence et structure) sont-elles clairement définies?

4. Une approche simplifiée: présentation

Le présent chapitre décrit le contenu d'une approche simplifiée d'évaluation des risques et de gestion des risques qui peut être utilisée par les PME à des fins d'auto-évaluation, ainsi que dans le cadre de projets d'externalisation, comme nous l'avons vu au chapitre 3.

La plupart des approches existantes d'évaluation et de gestion des risques liés à la sécurité sont généralement axées sur les besoins des grosses organisations. Une approche simple conçue à l'intention des petites organisations n'existe pas à ce jour, tout au moins sous la forme de recommandations disponibles au public. Certaines sociétés de conseil ont élaboré des bonnes pratiques à cet effet, mais elles les utilisent dans le cadre des projets clients. D'autres approches, bien qu'elles revendiquent d'être appropriées pour les PME, sont encore trop complexes pour des auto-évaluations (par exemple, OCTAVE). D'autre part, comme nous l'avons déjà mentionné, la plupart des PME n'ont pas les moyens de sous-traiter entièrement cette fonction à une tierce partie.

Nous avons l'intention de fournir à ces organisations une approche simple, efficace, et peu onéreuse pour identifier et gérer les risques liés à la sécurité de leur information. **L'approche simplifiée qui en résulte offre aux petites organisations les moyens d'effectuer une auto-évaluation. Elle est basée sur les principes, attributs et résultas d'OCTAVE[2], et adaptée aux environnements et besoins types des PME. En fait, cette approche est également compatible avec d'autres normes existantes, telles que la norme ISO 13335-2 par exemple.**

Pour une organisation cherchant à comprendre ses besoins en sécurité de l'information, la présente approche est une technique d'auto-évaluation et de planification de la sécurité basée sur le profil de risque. Contrairement aux évaluations axées sur la technologie, qui ciblent seulement le risque technologique, cette méthode cible le contexte et les risques inhérents et se concentre sur les questions pratiques d'ordre stratégique.

Le principal avantage de la présente approche réside dans le fait qu'elle peut fournir un niveau de sécurité acceptable en contrepartie d'un effort relativement peu important en matière d'évaluation et de gestion. Cela est dû aux aspects suivants qui facilitent son applicabilité:

- Le profil de risque de l'organisation peut être facilement identifié.
- Les actifs typiques des petites organisations sont connus.
- La protection des actifs à l'aide de mesures (contrôles) est définie au préalable à l'aide de cartes de contrôles.

Grâce à ces avantages, une auto-évaluation peu coûteuse peut être mise en œuvre par des équipes n'ayant qu'une faible expertise en matière de sécurité. Si elle est menée avec soin, elle débouchera sur un niveau de sécurité acceptable.

L'approche d'évaluation proposée peut être appliquée par des personnes non expertes. Lors d'une évaluation, l'équipe chargée de l'évaluation n'aura pas à faire face aux divers aspects des menaces auxquelles sont exposés des actifs vulnérables. On lui propose plutôt un niveau de protection prédéfini selon le type d'actif et le niveau de sécurité exigé.

Le travail effectué pour développer le modèle de risque sous-jacent à cette approche, est basé sur les suppositions et les éléments suivants:

- **Évaluation des risques inhérents** – L'environnement peut souvent définir le contexte de risque (risques inhérents) dans lequel évolue une entreprise. Par exemple, une petite entreprise spécialisée dans la cuisson au four a un contexte de risque nettement moins conséquent qu'une petite entreprise spécialisée dans les prestations de soins de santé ou dans les services de veille économique. Indépendamment de leurs mesures de sécurité, infrastructures et revenus, les deux entreprises évoluent dans des environnements de risque

[2] *Operationally Critical Threat, Asset, and Vulnerability Evaluation* et OCTAVE sont des marques de service de l'Université Carnegie Mellon. OCTAVE a été développée au centre de coordination de CERT (CERT/CC). Établie en 1988, cette équipe dédiée à la sécurité informatique est la plus ancienne qui existe.

totalement différents, ce qui doit être sérieusement pris en considération avant de définir la stratégie de sécurité de l'information et de choisir les contrôles de sécurité.

- **Variabilité des scénarios de menace (profils) observés dans les PME**. Dans le contexte des PME, malgré la variabilité normalement attendue au niveau des risques inhérents, nous avons néanmoins observé que les menaces sont plutôt typiques et que, dans la majorité des cas, elles peuvent être regroupées et former des profils de menaces génériques, applicables à un grand nombre de PME. À cet égard, notre travail vise à modéliser les menaces en utilisant des profils de menace génériques. Les profils de risque élaborés reflètent le niveau de risques inhérents d'une organisation. Les mesures ont été identifiées par la suite, et regroupées, afin de couvrir l'ensemble des menaces des profils de risques respectifs.

L'approche proposée est auto-gérée, ce qui signifie que les personnes d'une organisation assument la responsabilité d'évaluer les risques, de sélectionner les contrôles et de déterminer ainsi la stratégie de sécurité de l'organisation. Cette technique permet de décupler les connaissances qu'ont les personnes des pratiques et processus de leur entreprise en matière de sécurité pour **(a) appréhender l'état actuel des pratiques de sécurité au sein de l'organisation**, **(b) identifier les actifs les plus critiques, (c) hiérarchiser les domaines à améliorer et déterminer la stratégie de sécurité de l'organisation.** Cette démarche permettra de couvrir l'ensemble du cycle d'évaluation et de gestion des risques.

Quand la méthode proposée ici est appliquée, une petite équipe de personnes des unités opérationnelles (ou commerciales) et du département informatique travaillent ensemble pour répondre aux besoins en sécurité de l'organisation, en prenant en compte deux aspects majeur de la sécurité, à savoir, les mesures organisationnelles et les mesures basées sur les actifs.

Les organisations sont vivement encouragées à appliquer seulement à court terme les recommandations et les meilleures pratiques incluses dans cette approche, pour satisfaire l'objectif de protéger rapidement et efficacement les éléments essentiels et critiques de leur entreprise. Le contenu de cette approche couvre les risques importants auxquels les PME sont généralement exposées. Mais l'approche proposée n'est pas censée offrir une alternative définitive pour l'évaluation complète et détaillée des risques liés aux actifs critiques. Nous recommandons vivement une démarche plus approfondie pour mieux évaluer les risques, en particulier si des éléments complexes sont utilisés pour des actifs d'une très grande valeur.

Les objectifs motivant l'introduction de la présente approche d'évaluation et de gestion des risques sont les suivants:

- **Améliorer les seuils européens existants en matière de sécurité de l'information**. L'approche peut servir de catalyseur pour accélérer les efforts des PME en matière de gestion des risques liés à la sécurité de l'information en traitant les risques élevés. De surcroît, cibler les scénarios de menace types permettra d'améliorer les seuils européens existants en matière de sécurité de l'information.
- Satisfaire les besoins de l'entreprise et les contraintes caractéristiques des environnements de PME en **évitant une terminologie spécialisée et en éliminant les tâches très exigeantes** comprises dans quasiment toutes les méthodologies professionnelles et normes industrielles courantes disponibles sur le marché (c'est-à-dire, évaluation des actifs, analyse de l'impact sur l'entreprise, identification des exigences de sécurité, etc.).
- **Utiliser une approche auto-gérée** adaptée aux moyens, aux ressources et à l'expertise typiques de l'environnement des PME.
- **Se concentrer sur les actifs critiques et les risques les plus élevés**. La méthode a été développée sous la forme d'un guide simple d'usage qui permet d'identifier et de protéger les actifs jugés les plus critiques pour l'organisation.
- Développer une méthode d'évaluation et de gestion des risques **indépendante des mesures**. Afin d'obtenir un premier résultat pratique et réaliste, les contrôles d'OCTAVE ont été utilisés. Mais la méthode peut pratiquement utiliser tous les contrôles standard disponibles aujourd'hui (ISO, BS7799, NIST, BSI).

4.2 Hypothèses de travail

Outre les objectifs susmentionnés, quelques considérations/hypothèses ont été émises pour l'élaboration de ce guide et de l'approche d'évaluation des risques qu'il présente:

- Dans de nombreux cas, la PME n'est peut-être pas familiarisée avec la sécurité informatique et pourra donc tirer profit de l'accès au matériel de sensibilisation, formation et orientation.
- L'instauration d'un cadre d'orientation sur la sécurité par l'intermédiaire des associations et organismes professionnels des PME aidera à promouvoir la compréhension des questions de sécurité par les personnes peu familiarisées avec la sécurité de l'information.
- Les PME constituent un domaine prioritaire de la politique économique de l'UE et sont considérées comme des acteurs clés de la croissance socio-économique dans l'Union européenne.
- Les PME voient généralement le jour grâce à la passion entrepreneuriale de leur créateur mais ont un financement limité; elles forment souvent un ensemble disparate de systèmes internes, hétérogènes et indépendants.
- Les politiques et cadres de planification de la sécurité de l'information ainsi que les plans anti-sinistre sont généralement inexistants. De plus, les connaissances de base sur les risques liés à la sécurité de l'information se limitent souvent aux virus et logiciels antivirus.
- La plupart des dirigeants de PME ne comprennent guère la terminologie scientifique et technique complexe relative à la sécurité de l'information.
- Les petites entreprises travaillent généralement dans un cadre où l'environnement de traitement des données est normalisé, mais demeure important pour l'entreprise. Elles utilisent des progiciels grande distribution, consistant partiellement ou intégralement en des «boîtes noires» (avec tous les risques potentiels associés) et sont connectées à l'internet où se cachent de nombreuses menaces pour la sécurité informatique.
- Les menaces accidentelles comptent parmi les risques les plus élevés pour la sécurité de l'information des PME et pourtant les programmes de sensibilisation et de formation du personnel sont souvent négligés. Même si le personnel des PME a des connaissances spécifiques des systèmes d'information, il se peut qu'il n'ait pas de savoir-faire sur les questions de sécurité informatique. Par ailleurs, les entreprises ne peuvent généralement pas se permettre d'investir assez de ressources dans l'évaluation des risques et la gestion de risques ce qui constitue un facteur aggravant.

4.3 Approche en quatre phases

L'approche d'évaluation des risques proposée comprend **quatre phases** pour examiner les questions de sécurité liées à l'organisation et à la technologie, permettant ainsi de fournir une vision holistique complète des besoins en sécurité de l'information. Les quatre phases de la méthode sont illustrées à la figure 2.

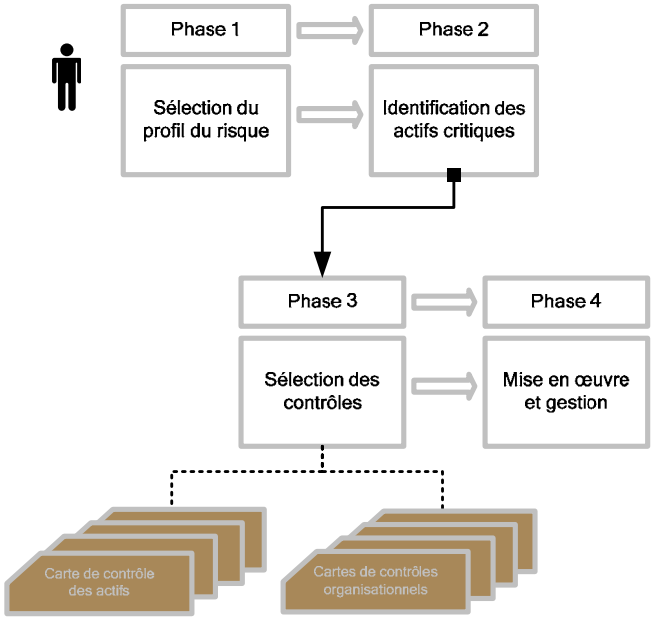

Figure 2: Les quatre phases sous-jacentes à l'approche d'évaluation des risques proposée

L'approche d'évaluation des risques est articulée autour de deux principaux aspects: **(1) le profil de risque de l'entreprise et (2) l'identification des actifs critiques**.

L'évaluation des risques est conduite par une petite équipe interdisciplinaire (trois à cinq personnes, membres du personnel de la PME, personnel extérieur ou une équipe mixte, selon le type d'évaluation choisi Comme cela a été dit au chapitre 3.3 Approches en matière de sécurité de l'information) qui se réunit, analyse les informations et élabore des plans de réduction des risques liés à la sécurité pour l'organisation. Pour effectuer l'évaluation des risques avec efficacité, l'équipe doit avoir une vaste connaissance des processus internes de l'organisation et de son infrastructure TI.

L'équipe d'analyse de la PME **utilisera comme point de départ le tableau d'évaluation du profil de risque afin d'identifier le profil de risque de l'entreprise.** L'étape suivante est **l'identification des actifs critiques de l'organisation** et les **exigences de sécurité appropriées** en termes de confidentialité, intégrité et disponibilité.

Les contrôles (cartes de contrôles) sont sélectionnés par la suite. Le processus de sélection est radicalement simplifié grâce à l'utilisation de cartes de contrôles standard. Les équipes clôturent le processus simplement en **se référant aux cartes de contrôles associées aux risques**, à la fois pour l'organisation et les actifs critiques identifiés, élaborées pour chaque niveau de profil de risque, catégorie d'actif et exigence en matière de sécurité (confidentialité, intégrité, disponibilité).

Les cartes de contrôles contiennent des contrôles provenant du catalogue des pratiques utilisé dans OCTAVE. Il en a été décidé ainsi parce que ces contrôles sont assez simples et plus facilement compris par des personnes non expertes en sécurité. Mais d'autres contrôles de sécurité peuvent être utilisés en alternative. C'est d'ailleurs nécessaire dans le cas où une PME dispose déjà d'une politique de sécurité basée sur une autre norme (par exemple, la norme ISO 17799).

À l'étape finale, l'équipe d'analyse de la PME s'occupe de hiérarchiser les actifs en fonction de leur criticité, de l'impact sur l'entreprise et du plan de protection.

Les paragraphes suivants décrivent les phases d'évaluation des risques de façon plus détaillée.

4.3.1 Phase 1 – Sélection du profil de risque

Durant cette phase, les équipes d'évaluation évaluent le profil de risque de l'entreprise en utilisant un ensemble prédéfini de **critères qualitatifs**. À l'aide du tableau d'évaluation du profil de risque (Tableau 2) les équipes d'évaluation sont en mesure d'identifier leur contexte de risque. Ce dernier est

déterminé à partir de l'entreprise et de l'environnement extérieur d'une organisation et peut être divisé en **quatre domaines de risque: juridique et réglementaire, renommée et confiance des clients, productivité, et stabilité financière**.

Domaine de risque	Élevé	Moyen	Faible
Juridique et réglementaire	L'organisation traite des informations client sensibles et personnelles, y compris des dossiers médicaux et des données personnelles critiques telles que définies par la législation communautaire en matière de protection des données.	L'organisation traite des informations client personnelles mais non sensibles telles que définies par la législation communautaire en matière de protection des données.	L'organisation ne traite pas des données personnelles autres que celles du personnel employé par l'organisation.
Productivité	L'organisation emploie plus de 100 salariés qui ont besoin d'accéder quotidiennement aux applications et services de l'entreprise.	L'organisation emploie plus de 50 salariés qui ont besoin d'accéder quotidiennement aux applications et services de l'entreprise.	L'organisation emploie moins de 10 salariés qui ont besoin d'accéder quotidiennement aux applications et services de l'entreprise.
Stabilité financière	Les revenus annuels de l'organisation dépassent 25 millions d'euros ou/et les transactions financières avec des tiers ou des clients font partie des activités courantes.	Les revenus annuels de l'organisation ne dépassent pas 25 millions d'euros.	Les revenus annuels de l'organisation ne dépassent pas 5 millions d'euros.
Renommée et perte de la confiance des clients	L'indisponibilité ou la qualité du service ont un impact direct sur les activités de l'organisation ou/et plus de 70% des clients accèdent en ligne aux produits et services de l'entreprise.	L'indisponibilité ou la qualité du service peuvent avoir un impact indirect sur les activités de l'organisation et/ou moins de 5% des clients accèdent en ligne aux produits et services de l'entreprise.	L'indisponibilité ou la qualité du service ne peuvent pas avoir d'impact direct ni indirect sur les activités de l'organisation ni entraîner une perte de revenus.

Tableau 2: Tableau d'évaluation du profil de risque

Chaque domaine de risque est décliné en trois classes (Élevé, Moyen et Faible) qui reflètent des critères quantitatifs pour l'organisation en question par rapport au domaine de risque et qui aident à identifier le niveau de risque. L'équipe évalue les risques identifiés pour chaque domaine afin d'élaborer le **profil de risque de l'organisation**.

Selon la méthode empirique, le plus haut risque identifié dans une classe de risque définit le profil de risque global de l'entreprise. Un risque élevé dans la classe de risque «stabilité financière» révèle un profil de risque élevé. De même, un risque moyen conduit à un profil de risque moyen et un risque faible à un profil de risque faible. Par exemple, un faible risque dans les classes «renommée et confiance des clients», «juridique et réglementaire» et «productivité», mais un risque élevé dans la classe de risque «stabilité financière», débouchent sur un profil de risque élevé.

La définition des profils de risque devrait être considérée comme une décision importante qui conduit à la sélection des actifs liés au risque et à leur protection par l'intermédiaire des cartes de contrôles.

4.3.2 Phase 2 – Identification des actifs critiques

Au cours de cette phase, l'équipe d'évaluation choisit les actifs critiques en fonction de l'importance relative de l'organisation et définit les prescriptions de sécurité de chaque actif critique.

La direction d'une organisation sait généralement quels sont ses **actifs clés** et peut consacrer ses ressources limitées à protéger ces actifs. L'équipe d'évaluation détermine ce qui est important pour

l'organisation (par exemple, les actifs en rapport avec l'information) et choisit les actifs qui sont les plus utiles pour l'organisation, qui sont également qualifiés d'**actifs critiques**.

Le tableau suivant définit les catégories d'actif, et les types d'actif pris en compte lors de la sélection des actifs critiques. Il s'agit de considérer en l'occurrence les actifs qui aident l'entreprise dans la conduite de ses activités. Certains types d'actif peuvent englober d'autres types d'actif. Par exemple, les composants d'une application peuvent être des serveurs, des postes de travail, des routeurs, des sections de réseau, etc.

Il convient de noter que la liste suivante, représentative de la plupart des petites entreprises, n'est pas exhaustive. Des actifs supplémentaires pourront être introduits sur demande (par exemple, dans les futures versions du présent document). En outre, il est possible qu'un type d'actif puisse utiliser d'autres actifs pour ses opérations. Par exemple, une application pourrait utiliser comme composants un serveur, quelques postes de travail, une mémoire et une section de réseau. Il faut noter qu'il ne suffit pas de protéger un actif, mais que chacun de ses composants doit également être protégé de façon appropriée.

Catégorie d'actif	Description	Actif (types)
Systèmes	Systèmes d'information qui traitent et stockent l'information. Les systèmes sont une combinaison d'actifs informationnels, de logiciels et de matériels. Tout ordinateur hôte, client, serveur, ou réseau peut être considéré comme un système. Les systèmes critiques sont ceux identifiés comme essentiels pour assurer la fourniture permanente de l'offre de services et de produits de l'entreprise, ceux qui stockent des informations internes critiques (informations client ou internes confidentielles) ou ceux qui sont exposés au monde extérieur pour des fonctions ou services commerciaux.	Serveur Ordinateur portable Poste de travail Archivage et secours informatique Mémoire
Réseau	Dispositifs importants pour les réseaux de l'organisation. Les routeurs, commutateurs et modems sont des exemples de cette classe de composants. Les composants/appareils sans fil, tels que les téléphones portables et les points d'accès sans fil que les membres du personnel utilisent pour accéder à l'information (par ex., courrier électronique). Les réseaux critiques sont généralement ceux qui sont utilisés à l'appui des applications ou systèmes critiques clés, ou ceux qui sont partagés avec une tierce partie et généralement les réseaux non fiables.	Routeurs Câblage Passerelles Points d'accès sans fil Section de réseau (par ex. câblage et équipement entre 2 ordinateurs) Autres (SAT, Laser)
Personne	Membres du personnel de l'organisation, ainsi que leurs compétences, formation, connaissances et expérience. Les personnes critiques sont celles qui jouent un rôle clé dans les processus opérationnels ou de production. Il faut accorder de l'importance aux ressources (humaines) critiques qui sont considérées comme irremplaçables ou qui constituent un point de défaillance unique.	Gestion des affaires et des ressources humaines Opérations et technologie Recherche et développement Ventes et marketing Contractants et tierces parties
Applications	Applications critiques. Les applications qui sont essentielles pour une partie ou l'ensemble de l'offre de produits et de services. L'arrêt des applications critiques entraîne généralement de graves entraves aux processus dépendants, voire même leur congestion.	Contrôle financier Assistance à la clientèle Logistique E-commerce Système ERP

Tableau 3: Liste des actifs

Lors de l'identification des actifs critiques, il est essentiel de considérer les avis des plus hauts dirigeants (ou du propriétaire de l'entreprise). La participation des plus hauts dirigeants à l'analyse garantit une bonne identification de la valeur des actifs informationnels.

Ensuite, il est nécessaire d'évaluer les prescriptions de sécurité des actifs les plus importants. Les prescriptions de sécurité révèlent les qualités d'un actif qui doivent être absolument protégées. Les prescriptions de sécurité examinées lors du processus d'évaluation sont les suivantes:

- confidentialité – nécessité de préserver la confidentialité d'informations faisant l'objet de droits de propriété, sensibles ou personnelles dont l'accès est réservé aux personnes autorisées;
- intégrité – authenticité, exactitude et intégralité d'un actif;
- disponibilité – propriété d'un actif qui consiste à être disponible au moment de son utilisation;

Les équipes d'évaluation devraient utiliser les critères de sélection des exigences tels que définis au tableau 4 afin d'identifier les principales prescriptions de sécurité pour les différentes catégories d'actif. Les exigences des actifs en matière de sécurité seront utilisées ultérieurement lors de la sélection des cartes de contrôles. Ce tableau a été élaboré comme un guide simple et pratique pour faciliter l'identification des critères de sécurité des actifs critiques sélectionnés antérieurement. Les prescriptions de sécurité mettent en lumière l'importance de l'actif et indiquent le niveau de protection nécessaire (par exemple, par l'utilisation de contrôles appropriés).

Le tableau suivant aidera les équipes d'évaluation à identifier les exigences de sécurité pour les différentes catégories d'actifs mentionnés ci-dessus.

Catégorie d'actif	Confidentialité	Intégrité	Disponibilité
Systèmes	Un système comportant des prescriptions de confidentialité traite souvent des informations comportant des données faisant l'objet de droits de propriété (R&D), des informations client, des données client sensibles d'ordre médical ou personnel.	Les systèmes comportant des prescriptions d'intégrité traitent généralement des transactions de nature financière, de l'achat de produits ou de commerce électronique.	Les prescriptions de disponibilité sont courantes dans les systèmes critiques pour les opérations quotidiennes d'une entreprise et lorsqu'un temps d'arrêt génère des coûts et frais généraux en termes d'affectation de ressources.
Réseau	Un réseau comportant des prescriptions de confidentialité couvre généralement des communications et échanges d'information dans des environnements non sécurisés et non fiables.	Il y a généralement des exigences d'intégrité pour un réseau lorsque des transactions ont lieu sur le réseau métropolitain partagé et public ou entre fournisseurs de télécommunication.	Les prescriptions de disponibilité sont particulièrement nécessaires lorsque le réseau est utilisé dans le cadre de l'assistance aux clients, ou de l'offre de produits et de services.
Personnes	Les prescriptions de confidentialité sont courantes lorsque les personnes traitent des informations confidentielles de l'organisation ou faisant l'objet de droits de propriété qui, si elles étaient divulguées, porteraient atteinte à l'image et à la clientèle de l'organisation.	Les prescriptions d'intégrité relatives aux personnes, concernent des secrets partagés tels que des clés cryptographiques ou des mots de passe. La possession de ce type de connaissance comporte des menaces relevant des facteurs humains qui devraient être prises en compte grâce à des contrôles correspondants.	Les prescriptions de disponibilité pour les actifs humains sont particulièrement importantes lorsque ces personnes sont des ressources critiques pour la continuité des opérations de l'offre de produits ou de services.
Applications	Les applications comportant des prescriptions de confidentialité traitent souvent des informations comportant des données faisant l'objet de droits de propriété (R&D), des informations client, des données client sensibles d'ordre médical ou personnel.	Les applications comportant des prescriptions d'intégrité traitent généralement des transactions de nature financière, de l'achat de produits ou de commerce électronique.	Les prescriptions de disponibilité sont satisfaites dans les applications qui sont critiques pour les opérations quotidiennes d'une entreprise et lorsqu'un temps d'arrêt génère des coûts et des frais généraux en termes de d'affectation de ressources.

Tableau 4: Tableau de sélection des prescriptions de sécurité

À l'issue de ce processus, les équipes d'évaluation devraient disposer d'un tableau des actifs critiques classés par catégorie d'actif et d'une liste des exigences correspondantes en matière de sécurité, ainsi que des informations à l'appui ou des justifications examinées lors de l'évaluation.

Ces résultats seront alors utilisés comme données d'entrée par la phase 3 – Sélection des cartes de contrôles, tel que décrit dans le chapitre suivant.

4.3.3 Phase 3 - Sélection des cartes de contrôles

Au cours de la phase 3, l'équipe d'évaluation sélectionne les contrôles appropriés en se basant sur le profil de risque choisi pour chaque catégorie de risque et sur la liste des actifs identifiés comme critiques (y compris leurs exigences). Les contrôles se divisent en deux catégories: contrôles organisationnels et contrôles basés sur les actifs.

L'ensemble de l'organisation est censée constituer un seul actif qui doit être protégé. Les contrôles de sécurité organisationnels ont généralement une large portée et s'appliquent à l'organisation de manière horizontale. Au contraire, les contrôles basés sur les actifs sont axés sur la mise en œuvre de la protection requise par les actifs (par exemple, faire respecter les règles sur la disponibilité d'un composant critique du réseau).

Les contrôles sont également regroupés par cartes de contrôles. Les équipes chargées de l'évaluation peuvent choisir entre deux cartes de contrôles:

- les cartes de contrôles qui comportent les contrôles applicables horizontalement à l'organisation et ayant trait aux pratiques et procédures de gestion, et
- les cartes de contrôles qui ciblent les actifs critiques et sont spécifiques à une catégorie d'actifs. Les cartes de contrôles sont principalement présélectionnées (les contrôles sont regroupés en fonction des profils de risque et des prescriptions de sécurité des actifs).

Le tableau 5 énumère les catégories de contrôle, leur structure et leur nom, tels qu'ils sont considérés dans cette approche. Comme cela a déjà été mentionné, nous avons adopté les contrôles de la méthode OCTAVE, en raison de leur simplicité. D'autres contrôles peuvent être utilisés à leur place (par exemple, des normes ISO 17799 ou IT-Grundschutz, etc.). Une description plus détaillée figure ci-après.

Catégorie de contrôle	Contrôle n°	Nom du contrôle
Organisationnel	**SP1**	Sensibilisation et formation à la sécurité
	SP2	Stratégie en matière de sécurité
	SP3	Gestion de la sécurité
	SP4	Politiques et règles de sécurité
	SP5	Gestion collaborative de la sécurité
	SP6	Plan d'urgence/plan anti-sinistre
Basé sur les actifs	**OP1.1**	Plans et procédures de sécurité
	OP1.2	Contrôle d'accès physique
	OP1.3	Surveillance et audit de la sécurité physique
	OP2.1	Gestion des systèmes et des réseaux
	OP2.2	Outils d'administration des systèmes
	OP2.3	Surveillance et audit de la sécurité des TI
	OP2.4	Authentification et autorisation
	OP2.5	Gestion des éléments vulnérables
	OP2.6	Cryptage

	OP2.7	Architecture et conception de la sécurité
	OP3.1	Gestion des incidents
	OP3.2	Pratiques générales du personnel

Tableau 5: Contrôles utilisés dans l'approche présentée

La phase 3 de l'approche d'évaluation proposée consiste donc en deux étapes distinctes mais d'égale importance:

- Étape A, Sélection des contrôles organisationnels
- Étape B, Sélection des contrôles basés sur les actifs

Au cours de ces étapes, les contrôles sont affectés à l'organisation (sous la forme d'un seul actif important) et aux actifs critiques identifiés comme indiqué ci-dessous.

Sélection des cartes de contrôles organisationnels

La sélection des cartes de contrôles organisationnels est effectuée de façon assez directe: des contrôles organisationnels sont disponibles pour chaque profil de risque (défini dans la matrice des profils de risque). Le tableau suivant attribue des contrôles organisationnels aux profils de risque tels que mentionnés au chapitre 4.3.1 Phase 1 – Sélection du profil de risque. Les contrôles énumérés ci-dessous sont recommandés afin de réduire les risques organisationnels respectifs. Une description détaillée des contrôles figure à l'Annexe C. Contrôles organisationnels.

Domaines de risque	**Élevé**	**Moyen**	**Faible**
Juridique et réglementaire	(SP1) (SP4)	(SP1) (SP4)	SP1.1
Productivité	(SP3) (SP4) (SP6) (SP5)	(SP4) (SP6)	SP4.1
Perte financière	(SP2) (SP1) (SP4)	(SP4)	SP4.1
Renommée et perte de confiance des clients	(SP1) (SP5)	(SP4) (SP1)	SP4.1

Tableau 6: Cartes de contrôles organisationnels

Sélection des cartes de contrôles basés sur les actifs

En se basant sur le profil de risque et les exigences de sécurité des actifs, les équipes d'évaluation des PME peuvent utiliser le tableau des cartes de contrôles basés sur les actifs (voir tableau 7) afin d'identifier les contrôles appropriés pour la protection des actifs critiques.

Cartes de contrôles basés sur les actifs			
Actif	**Cartes de risque élevé**	**Cartes de risque moyen**	**Cartes de faible risque**
Application	**CC-1A**	**CC-2A**	**CC-3A**
Système	**CC-1S**	**CC-2S**	**CC-3S**
Réseau	**CC-1N**	**CC-2N**	**CC-3N**
Personnes	**CC-1P**	**CC-2P**	**CC-3P**

Tableau 7: Cartes de contrôles des actifs

Les cartes de contrôles basés sur les actifs sont principalement regroupées dans les trois catégories suivantes: profil de risque organisationnel, catégorie d'actif et exigence en matière de sécurité. Par exemple, les équipes d'évaluation confrontées à un profil de risque élevé auront différentes prescriptions de sécurité que si elles avaient affaire à des profils de risque moyen ou faible. Chaque carte de contrôles implique un certain nombre de contrôles d'actifs (voir Annexe B. Cartes de contrôles des actifs) pour traiter l'éventail complet des risques et des prescriptions de sécurité tel que cela est requis par le profil particulier et édicté par les exigences choisies en matière de sécurité. Une description plus détaillée des contrôles inclus dans les cartes de contrôles figurent à l'annexe D, Contrôles basés sur les actifs.

Pour les besoins de cette présentation, nous ajoutons à ce stade la carte de contrôles CC-1A, qui comme indiqué dans le tableau ci-dessous, est appropriée pour la protection d'une application dans un scénario à haut risque (profil de risque élevé).

ID carte de contrôles basés sur les actifs					**CC-1A**					
Profil de risque	**Élevé**									
Catégorie d'actif	**Application**									
Prescriptions de sécurité	**Sécurité physique**	**Gestion des systèmes et des réseaux**	**Outils d'administration des systèmes**	**Surveillance et audit de la sécurité des TI**	**Authentification et autorisation**	**Gestion des éléments vulnérables**	**Cryptage**	**Architecture et conception de la sécurité**	**Gestion des incidents**	**Pratiques générales du personnel**
Confidentialité		2.1.3			2.4.2	2.5.1	2.6.1			
Intégrité		2.1.4			2.4.2	2.5.1	2.6.1			
Disponibilité		2.1.6								

Tableau 8: Exemple d'une carte de contrôles pour une application dans un profil à haut risque

À l'aide des exigences identifiées antérieurement en matière de sécurité et de la carte de contrôles, les équipes d'évaluation peuvent ensuite identifier des contrôles plus spécifiques (par exemple, les contrôles pour la disponibilité, la confidentialité ou l'intégrité). Il convient de noter que dans le cas où plus d'une exigence est sélectionnée, les contrôles applicables à l'actif correspondent à la somme des contrôles pour chaque exigence.

4.3.4 Phase 4 – Mise en œuvre et gestion

Lors de la phase 4 et sur la base des informations évaluées, l'équipe d'évaluation élabore des plans de réduction des risques auxquels les actifs critiques sont exposés.

Après l'identification (1) du profil de risque de l'organisation, (2) des actifs critiques et (3) des cartes de contrôles, l'équipe d'évaluation planifie la mise en œuvre des contrôles sélectionnés. En raison de leurs ressources limitées, les PME ne seront sans doute pas en mesure de mettre en œuvre en une

seule fois tous les contrôles identifiés pour tous les actifs critiques. À cet égard, la hiérarchisation est un élément indispensable pour assurer le succès des efforts de réduction des risques.

Un plan de mise en œuvre définit de quelle façon une organisation a l'intention de maintenir ou d'accroître le niveau existant de sécurité. Son objectif est de définir une orientation pour les efforts à venir en matière de sécurité de l'information, plutôt que de trouver une solution immédiate à chaque problème de sécurité et vulnérabilité.

Quelques critères sont indiqués ci-après qui permettent de hiérarchiser les actions pour mettre en œuvre les cartes de contrôles identifiées. Ils ne sont pas tous applicables dans toutes les entreprises. Cela peut néanmoins servir de guide générique:

- **Alignement stratégique sur les buts de l'organisation**: cet actif soutient-il directement les buts du plan de travail établis par écrit de la division et/ou de l'organisation? Quels buts et/ou objectifs du plan de travail seront soutenus et de quelle façon?
- **Efforts d'amélioration continue**: cet actif soutient-il un effort d'amélioration continue de la division? Quel est l'actif d'amélioration continue? Comment cet actif soutient-il les buts d'amélioration continue?
- **Mandats juridiques ou réglementaires**: si un actif doit satisfaire des exigences réglementaires, cela se reflétera dans la définition des priorités.
- **Avantages à l'échelle du système**: les avantages à l'échelle du système incluent l'amélioration du service à la clientèle pour plusieurs groupes de clients. Une plus grande priorité sera donnée aux groupes de clients jugés critiques, mais plus le groupe de clients concernés sera conséquent, plus l'avantage sera important.
- **Économies de coûts/temps**: les estimations d'économies de coûts et/ ou de temps incluent le temps du personnel, les économies de temps des clients, la génération de revenus, et les réductions directes de budget/coûts.
- **Réduction des risques**: suite à un projet, l'information et/ou les services empêcheront les pertes de revenus et/ou la non conformité aux politiques, et aux exigences juridiques et en matière d'audit.

La prochaine étape est le processus de planification, qui indique et surveille le calendrier précis de mise en œuvre des procédures et des outils de sécurité.

La question clé qui revient dans presque tous les projets des PME dans ce domaine est de savoir si les ressources internes sont adéquates ou capables de réaliser le plan de mise en œuvre. En d'autres termes, il conviendrait de prendre une décision quant à l'internalisation ou l'externalisation des tâches associées de gestion et de mise en œuvre.

5. Conseils pour l'auto-évaluation avec deux exemples

Dans ce chapitre, une décomposition plus détaillée des quatre phases sera présentée en étapes logiques, ceci avant d'aider les PME à (1) identifier le profil de risque de leur organisation, (2) identifier les actifs critiques qui doivent être sécurisés, (3) sélectionner les contrôles et les solutions visant à améliorer la sécurité et enfin (4) développer les plans d'amélioration. Toutefois, les actions et solutions qui peuvent être appliquées aux PME ne sont pas uniquement limitées à celles fournies ici.

De nouveau, les organisations sont vivement encouragées à suivre les conseils et les meilleures pratiques figurant dans cette méthode uniquement à court terme, et dans le but de protéger rapidement et efficacement les composants critiques de leur entreprise. Mais ce processus n'est pas censé remplacer une approche d'évaluation des risques complète et approfondie, qui est largement recommandée comme point de départ pour une stratégie de gestion des risques à long terme.

Avant de commencer à utiliser cette méthode, les PME doivent comprendre les trois aspects uniques qui les caractérisent:

- Une petite équipe d'analyse interdisciplinaire de trois ou cinq personnes conduit le processus d'évaluation des risques. Collectivement, les membres de l'équipe d'analyse doivent avoir une vision d'ensemble des affaires et des processus de sécurité de l'organisation, suffisante pour réaliser toutes les activités d'évaluation des risques. Pour cette raison, la méthode n'exige pas d'atelier de collecte de données pour entreprendre l'évaluation.
- La méthode prévoit une exploration limitée de l'infrastructure informatique. Puisque les petites organisations externalisent souvent leurs services et fonctions de TI, elles n'ont généralement pas développé les capacités organisationnelles pour exécuter et interpréter les résultats des outils d'évaluation de la vulnérabilité. Toutefois, même si elle ne dispose pas de ces capacités organisationnelles, une entreprise peut instaurer une stratégie de protection.
- Plutôt que d'utiliser les données de vulnérabilité pour améliorer sa vision de ses pratiques courantes en matière de sécurité, une organisation effectuant une évaluation examine les processus employés pour configurer et maintenir son infrastructure informatique dans des conditions de sécurité.

Le document est structuré, de façon modulaire, en phases et étapes. Deux exemples sont fournis pour chaque phase. Les exemples utilisent les scénarios d'entreprise suivants:

- **Entreprise de l'exemple A.** Dans l'exemple A, nous considérons le cas spécial d'un service de soins médicaux, de moyenne importance, qui assure un soutien en ligne aux médecins qui ont besoin de conseils pour leurs patients et d'informations concernant les avancées de la médecine. La base de données à l'appui de cette application stocke des données critiques et confidentielles de nature personnelle. La société emploie 100 personnes et a trois départements, le département de soutien médical et pharmaceutique, le département des sciences médicales et le département de gestion qui englobe les activités concernant les ressources humaines et le contrôle financier.
- **Entreprise de l'exemple B.** La société de l'exemple B est un petit cabinet d'avocats. Dans ce type de société, les systèmes informatiques sont largement utilisés pour stocker des informations sur les affaires, échanger des courriers électroniques et préparer et traiter les documents nécessaires. Le cabinet emploie cinq avocats et une secrétaire.

Les figures (organigrammes) sont fournies pour chaque phase; des allusions à la mise en œuvre sont faites pour chaque étape dans les encadrés en pointillés, pour chacune des descriptions de phase.

Phase 1 – Sélectionner le profil de risque

L'équipe d'analyse considère quels éléments de risque, au niveau de la protection de l'information, sont susceptibles (a) d'affecter ou de compromettre directement ou indirectement la renommée de l'organisation et la confiance des clients, (b) d'entraîner une non conformité juridique et réglementaire, (c) de créer des pertes financières (d) de diminuer la productivité. Elle sélectionne ensuite un niveau de risque approprié pour chaque domaine de risque à l'aide du tableau d'évaluation du profil de risque. Les domaines spécifiés sont les suivants: juridique et réglementaire, productivité, stabilité financière, renommée et perte de la confiance des clients. Comme le montre la figure 3, la phase comprend deux étapes.

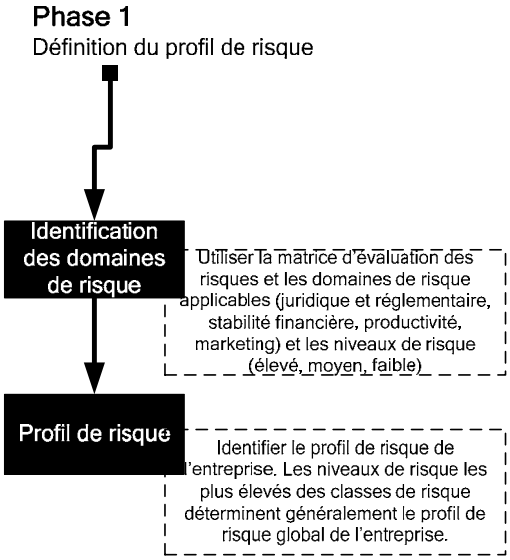

Figure 3: Phase 1 – Processus de sélection du profil de risque

Pour identifier le niveau de risque actuel ou potentiel, les membres de l'équipe d'analyse devraient mettre en évidence le domaine de risque et lire la description dans chaque colonne. Les domaines de risque qui sont les plus proches de leur profil d'entreprise, sont choisis. Le processus est suivi pour chaque domaine de risque. Au final, il devrait y avoir une MATRICE indiquant le niveau de risque applicable dans chaque domaine de risque.

Exemple A. (profil de risque élevé)

Dans l'exemple A, l'équipe utilise le **tableau d'évaluation du profil de risque** pour identifier le contexte de la société. L'équipe identifie un niveau de risque élevé (représenté en rouge) dans le domaine «juridique et réglementaire» puisque la société traite des informations sensibles de nature personnelle. Dans le même temps, elle trouve un niveau de risque élevé dans la «productivité», étant donné qu'elle emploie 100 personnes, un niveau de risque moyen (représenté en orange) dans la «stabilité financière» et un faible niveau de risque (représenté en bleu) dans le domaine «renommée et perte de confiance des clients» comme indiqué dans le tableau d'évaluation du profil de risque ci-après.

Domaines de risque	Élevé	Moyen	Faible
Juridique et réglementaire	**L'entreprise traite des informations client sensibles et personnelles, y compris des dossiers médicaux et des données personnelles telles que définies par la législation communautaire en matière de protection des données.**	L'entreprise traite des informations client personnelles mais non sensibles telles que définies par la législation communautaire en matière de protection des données.	L'entreprise ne traite pas des données personnelles autres que celles du personnel employé par l'organisation.
Productivité	**L'entreprise emploie plus de 100 personnes qui ont besoin d'accéder quotidiennement aux applications et services de l'entreprise.**	L'entreprise emploie plus de 50 personnes qui ont besoin d'accéder chaque jour aux applications et services de l'entreprise.	L'entreprise emploie moins de 10 salariés qui ont besoin d'accéder quotidiennement aux applications et services de l'entreprise.
Stabilité financière	Les revenus annuels dépassent 25 millions d'euros ou/ et les transactions financières avec des tiers ou des clients font partie des activités courantes.	**Les revenus annuels ne dépassent pas 25 millions d'euros**	Les revenus annuels ne dépassent pas 5 millions d'euros.
Renommée et perte de confiance des clients	L'indisponibilité ou la qualité du service ont un impact direct sur le profil de l'organisation ou/et plus de 70% des clients accèdent en ligne aux produits et services de l'entreprise.	L'indisponibilité ou la qualité peuvent avoir un impact indirect sur le profil de l'entreprise et/ou moins de 5% des clients accèdent en ligne aux produits et services de l'entreprise.	**L'indisponibilité ou la qualité du service ne peuvent pas avoir d'impact direct ni indirect sur le profil de l'entreprise ni entraîner une perte de revenus.**

Tableau 9: Tableau d'évaluation du profil de risque - Exemple A

Ensuite le profil de risque de l'entreprise est calculé. Les domaines de risques couvrent le contexte de risque global de l'entreprise. **Il est recommandé que le profil de risque soit équivalent au plus haut niveau identifié dans les domaines de risque subordonnés de la matrice de risques.**

Le tableau ci-dessous illustre les niveaux de risque identifiés dans les domaines de risque prédéfinis et indique où l'organisation devrait concentrer ses efforts pour appliquer des contrôles appropriés de la sécurité. Le tableau peut être utilisé pour établir les priorités également. Les niveaux de risque élevés indiquent un besoin urgent d'amélioration tandis que des niveaux de risque faibles mettent en évidence les actions qui devraient être prises en considération pour les améliorations à venir.

Domaines de risque	Niveau de risque	Profil de risque
Juridique et réglementaire	**Élevé**	**Élevé**
Productivité	**Élevé**	
Stabilité financière	**Moyen**	
Renommée et perte de confiance des clients	**Faible**	

Tableau 10: Profil de risque de l'organisation - Exemple A

Exemple B. (profil de risque moyen)

Dans l'exemple B, l'équipe utilise le **tableau d'évaluation du profil de risque** pour identifier le contexte de la société. L'équipe d'analyse identifie un faible niveau de risque (représenté en bleu) dans le domaine «juridique et réglementaire», étant donné que l'entreprise ne traite pas des données personnelles autres que celles des personnes employées par l'organisation, un faible niveau de risque dans la «productivité» (représenté en bleu), un faible niveau de risque dans la «stabilité financière» (représenté en bleu) et un niveau de risque moyen (représenté en orange) dans le domaine «renommée et perte de confiance des clients», comme indiqué dans le tableau d'évaluation du profil de risque ci-après.

Domaines de risque	Élevé	Moyen	Faible
Juridique et réglementaire	L'entreprise traite des informations client sensibles et personnelles, y compris des dossiers médicaux et données personnelles critiques telles que définies par la législation communautaire en matière de protection des données.	L'entreprise traite des informations client personnelles mais non sensibles telles que définies par la législation communautaire en matière de protection des données.	**L'entreprise ne traite pas des données personnelles autres que celles du personnel employé par l'organisation.**
Productivité	L'entreprise emploie plus de 100 salariés qui ont besoin d'accéder quotidiennement aux applications et services de l'entreprise.	L'entreprise emploie plus de 50 salariés qui ont besoin d'accéder quotidiennement aux applications et services de l'entreprise.	**L'entreprise emploie moins de 10 salariés qui ont besoin d'accéder quotidiennement aux applications et services.**
Stabilité financière	Les revenus annuels de l'organisation dépassent 25 millions d'euros ou/ et les transactions financières avec des tiers ou des clients font partie des activités courantes.	Les revenus annuels ne dépassent pas 25 millions d'euros.	**Les revenus annuels de l'organisation ne dépassent pas 5 millions d'euros**
Renommée et perte de confiance des clients	L'indisponibilité ou la qualité du service ont un impact direct sur le profil de l'organisation ou/et plus de 70% des clients accèdent en ligne aux produits et services de l'entreprise.	**L'indisponibilité ou la qualité du service peut avoir un impact indirect sur le profil de l'entreprise et/ou moins de 5% des clients accèdent en ligne aux produits et services de l'entreprise.**	L'indisponibilité ou la qualité du service ne peuvent pas avoir d'impact direct ni indirect sur le profil de l'entreprise ni entraîner une perte de revenus.

Tableau 11: Tableau d'évaluation du profil de risque- Exemple B

Ensuite, le profil de risque de l'entreprise est calculé. Les domaines de risque révélateurs du contexte de risque global de l'entreprise. **Il est recommandé que le profil de risque soit équivalent au plus haut niveau identifié dans les domaines de risque subordonnés de la matrice de risques.**

Le tableau ci-dessous illustre les niveaux de risque identifiés dans les domaines de risque prédéfinis et indique où l'organisation devrait concentrer ses efforts pour appliquer des contrôles appropriés de la sécurité. Le tableau peut être utilisé pour établir les priorités également. Les niveaux de risque élevés indiquent un besoin urgent d'amélioration tandis que des niveaux de risque faibles mettent en évidence les actions qui devraient être prises en considération pour les améliorations à venir.

Domaines de risque	Niveau de risque	Profil de risque
Juridique et réglementaire	**Faible**	**Moyen**
Productivité	**Faible**	
Stabilité financière	**Faible**	
Renommée et perte de la confiance des clients	**Moyen**	

Tableau 12: Profil de risque de l'organisation – Exemple B

Phase 2 – Identifier les actifs critiques

La phase 2 exige des décisions qui déterminent le restant de l'évaluation — à travers la sélection des actifs critiques de l'organisation. Selon la taille de l'organisation, le nombre d'actifs informationnels identifiés lors de cette phase pourrait facilement dépasser une centaine. Pour que l'analyse soit gérable, les PME doivent réduire l'étendue de l'évaluation en choisissant les quelques actifs qui sont les plus critiques pour mener à bien la mission et les objectifs de l'organisation. Seuls ces actifs seront analysés lors des activités ultérieures. Comme le montre la figure 4, la phase 2 comprend trois étapes.

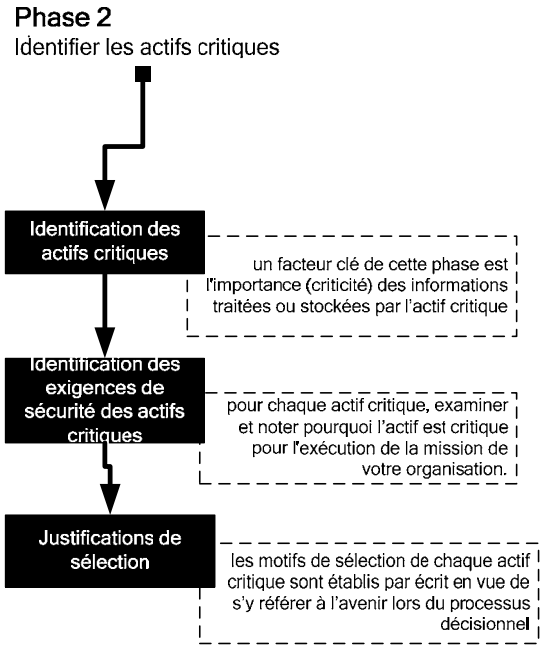

Figure 4: Phase 2 – Processus d'identification des actifs critiques

Étape 1. Sélectionner les cinq actifs les plus critiques de votre organisation

Lors de la sélection des actifs critiques, les équipes ne sont pas limitées à seulement cinq actifs, même si ce nombre est normalement suffisant pour permettre aux organisations de développer un ensemble de plans de réduction des risques lors de la phase 4. Les membres de l'équipe d'analyse doivent juger par eux-mêmes s'il convient d'en utiliser plus ou moins que cinq. Lors du processus de sélection des actifs critiques, les membres de l'équipe devraient examiner quels actifs entraîneront un fort impact négatif sur l'organisation dans l'un des scénarios suivants:

- **Divulgation** d'information à des personnes non autorisées
- **Modification** de l'information sans autorisation
- **Perte ou destruction** de l'actif

- **Accès interrompu** à l'actif ou à l'information stockée

Si les actifs critiques s'avèrent difficiles à identifier, les équipes devraient considérer les fonctions internes/ domaines au sein de l'organisation. Il pourrait s'agir de différents projets, groupes de travail (groupes de personnes avec différentes descriptions de poste) ou même de départements distincts de l'organisation (départements des RH, comptable, marketing, des ventes, etc.). Ces actifs devraient alors être énumérés par niveau d'importance pour le processus d'entreprise. Après avoir défini les domaines qui doivent être sécurisés, ou après avoir réorganisé les actifs de l'organisation, l'étape suivante est d'énumérer tous les actifs selon leur impact sur le processus d'entreprise. À cet effet, une méthode plus simple consiste à regrouper les actifs par département ou par fonction.

Un facteur clé lors de l'identification des actifs critiques est l'importance (criticité) de l'information traitée ou stockée par l'actif critique. En effectuant l'analyse de décomposition, les membres de l'équipe peuvent facilement identifier où et comment sont stockées ou utilisées les informations critiques.

Étape 2. Noter les justifications de la sélection de chaque actif critique

Au cours de la sélection des actifs critiques à l'étape 1, un certain nombre de questions en rapport avec ces actifs sont débattues. Dans cette étape, les motifs de sélection de chaque actif critique sont établis par écrit en vue de s'y référer à l'avenir lors du processus décisionnel. En outre, comprendre les raisons pour lesquelles un actif est critique permet de mieux définir les exigences de sécurité au cours de l'étape suivante. Pour chaque actif critique, les questions suivantes devraient être examinées et les réponses notées:

- Pourquoi l'actif est-il critique pour l'exécution de la mission de l'organisation?
- Qui le contrôle?
- Qui en est responsable?
- Qui l'utilise?
- Comment est-il utilisé?

Ces questions sont axées sur la façon dont les actifs sont utilisés et sur les raisons pour lesquelles ils sont importants. Si des réponses ne sont pas apportées à toutes ces questions, les personnes de l'organisation qui sont en mesure de fournir les réponses doivent être identifiées et incluses dans l'équipe d'analyse. L'information générée dans le cadre de la démarche de réponse à ces questions, sera utile ultérieurement dans ce processus. À cet égard, il convient de prendre soigneusement note des informations collectées ici.

Étape 3. Identifier les prescriptions de sécurité des actifs critiques

En général, pour décrire une exigence d'un actif en matière de sécurité, il faut comprendre quel aspect de l'actif est important. Pour les actifs informationnels, les prescriptions de sécurité sont généralement axées sur la confidentialité, l'intégrité et la disponibilité de l'information.

Les prescriptions de sécurité peuvent varier pour différentes catégories d'actif au sein d'une PME, mais une sélection attentive des exigences est essentielle pour la tâche suivante, à savoir, la sélection des contrôles. En d'autres termes, si une importante disponibilité de l'actif est exigée, la même exigence s'imposera au niveau des contrôles, etc.

Les équipes d'analyse utilisent les **critères de sélection des exigences,** comme prévu, afin d'identifier les exigences les plus importantes en matière de sécurité. **Les exigences des actifs en matière de sécurité seront utilisées ultérieurement au cours de la sélection des cartes de contrôles des actifs.** Les critères d'évaluation des prescriptions de sécurité ont été élaborés sous la forme d'un guide pratique, simple d'utilisation, pour évaluer les exigences de sécurité en termes de confidentialité, intégrité et disponibilité des actifs critiques sélectionnés. L'évaluation met en évidence

l'importance des attributs de sécurité des actifs et indique les contrôles appropriés pour assurer leur protection.

En guise de résultat, les équipes devraient avoir **un tableau énumérant les actifs critiques ainsi qu'une brève description de leur importance pour l'accomplissement de la mission de l'entreprise, les éléments de base et les prescriptions de sécurité**.

Pour les trois étapes décrites ci-dessus, les tableaux du paragraphe 4.3.2 peuvent être utilisés pour identifier les actifs appropriés et leurs exigences (voir Tableau 3 et Tableau 4).

Exemple A. (profile de risque: élevé, actif critique: application - phase 2.)

[Étape 1] Dans l'exemple A, l'actif identifié comme le plus critique est l'application Web fournissant un support en ligne aux clients (médecins). Cette application est essentielle pour l'entreprise dans la mesure où elle représente l'élément le plus important de l'offre de services, et elle est donc choisie comme l'actif le plus critique.

[Étape 2] Dans l'étape suivante les membres de l'équipe consignent les éléments qui constituent l'actif ainsi que les justifications de leur choix. Ainsi, ils identifient finalement comme éléments essentiels de l'actif la base de données qui stocke les informations client, la section de réseau qui supporte la connectivité avec les réseaux internes et externes, le serveur web et les murs pare-feux.

[Étape 3] Ensuite, les prescriptions de sécurité sont identifiées. En utilisant le tableau suivant (Tableau 13), les équipes reconnaissent les cases qui correspondent à leurs exigences. Dans l'exemple A, l'équipe sélectionne la base de données pour avoir les exigences relatives à la confidentialité puisque les données stockées concernent les clients de la société, elle sélectionne le réseau pour avoir les exigences relatives à la disponibilité et la confidentialité, puisque le réseau transmet des informations qui doivent rester intactes et être tenues secrètes pour effectuer des transactions ou interrogations.

Actifs	Confidentialité	Intégrité	Disponibilité
Systèmes	Un système comportant des prescriptions de confidentialité traite souvent des informations qui incluent des données faisant l'objet de droits de propriété (R&D), des informations client, des données client sensibles d'ordre médical ou personnel.	Un système comportant des prescriptions d'intégrité traite généralement des transactions de nature financière, de l'achat de produits ou de commerce électronique.	Les prescriptions de disponibilité sont satisfaites dans les systèmes critiques pour les opérations quotidiennes d'une entreprise et lorsqu'un temps d'arrêt génère des coûts et frais généraux en termes d'affectation de ressources.
Réseau	Un réseau comprenant des prescriptions de confidentialité couvre généralement des communications et échanges d'information dans des environnements non sécurisés et non fiables.	Les prescriptions d'intégrité sont particulièrement nécessaires lorsque des transactions se déroulent sur le réseau métropolitain partagé et public ou entre les fournisseurs de télécommunication.	Les prescriptions de disponibilité sont particulièrement nécessaires lorsque le réseau est utilisé dans le cadre de l'assistance aux clients ou de l'offre de produits et de services.
Personnes	Les prescriptions de confidentialité sont courantes lorsque les personnes traitent des informations confidentielles de l'entreprise ou faisant l'objet de droits de propriété qui, si elles étaient divulguées, porteraient atteinte à l'image et à la clientèle de l'organisation.	Les prescriptions d'intégrité relatives aux personnes concernent des secrets partagés tels que des clés cryptographiques ou des mots de passe. La possession de ce type de connaissance comporte des menaces relevant de facteurs humains qui devraient être prises en compte grâce à des contrôles correspondants.	Les prescriptions de disponibilité pour les actifs humains sont particulièrement importantes lorsque ces personnes constituent des ressources critiques pour la continuité des opérations de l'offre de produits ou de services.
Applications	**Les applications comprenant des prescriptions de confidentialité traitent souvent des informations qui incluent des données faisant l'objet de droits de propriété (R&D), des informations client, des données client d'ordre médical ou personnel.**	**Les applications comprenant des prescriptions d'intégrité traitent généralement des transactions de nature financière, de l'achat de produits ou de commerce électronique.**	**Les prescriptions de disponibilité sont satisfaites dans les applications qui sont critiques pour les opérations quotidiennes d'une entreprise et lorsqu'un temps d'arrêt génère des coûts et frais généraux en termes d'affectation de ressources.**

Tableau 13: Tableau de sélection des prescriptions de sécurité – Exemple A

En guise de résultat, les équipes d'analyse élaborent un tableau énumérant les actifs critiques ainsi que les justifications de leur sélection, les éléments de base et les prescriptions de sécurité pour les services fournis. Le tableau ci-dessous est le résultat de l'exemple A pour la phase 1 (voir Tableau 14).

Actif critique	Catégorie d'actifs	Composants	Prescriptions de sécurité	Justification de la sélection
Application du commerce électronique	Application	Base de données Mur pare-feu Section du réseau Serveur	**Confidentialité** **Intégrité** **Disponibilité**	L'application est essentielle pour l'entreprise car elle représente l'élément le plus important de l'offre de services.

Tableau 14: Justifications des prescriptions de sécurité

Exemple B. (profil de risque: moyen, actif critique: système – phase 2.)

[Étape 1] Dans l'exemple B, les actifs identifiés comme les plus critiques sont les postes de travail utilisés pour effectuer les activités quotidiennes, y compris la correspondance avec les clients, les informations client concernant les affaires et les informations comptables de base concernant les factures et les créances.

[Étape 2] Dans l'étape suivante, les membres de l'équipe consignent les éléments qui constituent l'actif ainsi que les justifications de leur choix. Ainsi, ils identifient quatre postes de travail, le réseau interne et le serveur de fichiers.

[Étape 3] Ensuite, les prescriptions de sécurité sont identifiées. En utilisant le tableau suivant, les équipes reconnaissent les cases qui correspondent à leurs exigences. Dans l'exemple B, l'équipe sélectionne les postes de travail avec les prescriptions de disponibilité, car ces derniers, utilisés pour les activités quotidiennes de l'entreprise, doivent rester opérationnels.

Actifs critiques	Confidentialité	Intégrité	Disponibilité
Systèmes	Un système comportant des prescriptions de confidentialité traite souvent des informations comportant des données faisant l'objet de droits de propriété (R&D), des informations client, des données client sensibles d'ordre médical ou personnel.	Un système comportant des prescriptions d'intégrité traite généralement des transactions de nature financière, de l'achat de produits ou de commerce électronique.	**Les prescriptions de disponibilité sont satisfaites dans les systèmes critiques pour les opérations quotidiennes d'une entreprise et lorsqu'un temps d'arrêt génère des coûts et frais en termes d'affectation de ressources.**
Réseau	Un réseau comportant des prescriptions de confidentialité couvre généralement des communications et échanges d'information dans des environnements non sécurisés et non fiables.	Les prescriptions d'intégrité sont particulièrement nécessaires lorsque des transactions ont lieu sur le réseau métropolitain partagé et public ou entre les fournisseurs de télécommunication.	Les prescriptions de disponibilité sont particulièrement nécessaires lorsque le réseau est utilisé dans le cadre de l'assistance aux clients, ou de l'offre de produits et de services.
Personnes	Les prescriptions de confidentialité sont courantes lorsque les personnes traitent des informations confidentielles de l'entreprise ou faisant l'objet de droits de propriété qui, si elles étaient divulguées, porteraient atteinte à l'image et à la clientèle de l'organisation.	Les prescriptions d'intégrité relatives aux personnes, concernent des secrets partagés tels que des clés cryptographiques ou des mots de passe. La possession de ce type de connaissance comporte des menaces relevant des facteurs humains qui devraient être prises en compte grâce à des contrôles correspondants.	Les prescriptions de disponibilité pour les actifs humains sont particulièrement importantes lorsque ces personnes sont des ressources critiques pour la continuité des opérations de l'offre de produits ou de services.
Applications	Les applications comportant des prescriptions de confidentialité traitent souvent des informations comportant des données faisant l'objet de droits de propriété (R&D), des informations client, des données client d'ordre médical ou personnel.	Les applications comportant des prescriptions d'intégrité traitent généralement des transactions de nature financière, de l'achat de produits ou de commerce électronique.	Les prescriptions de disponibilité sont satisfaites dans les applications qui sont essentielles pour les opérations quotidiennes d'une entreprise et lorsqu'un temps d'arrêt génère des coûts et frais généraux en termes d'affectation de ressources.

Tableau 15: Tableau de sélection des prescriptions de sécurité – Exemple B

En guise de résultat, les équipes d'analyse élaborent un tableau énumérant les actifs critiques ainsi que les justifications de leur sélection, les éléments de base, et les prescriptions de sécurité pour les services fournis. Le tableau ci-dessous est le résultat de l'exemple B de l'étape 3 (Tableau 16).

Actif critique	Type d'actif	Composants	Exigence en matière de sécurité	Justification de la sélection
Postes de travail	**Système**	**4 postes de travail** **Section de réseau** **Serveur**	**Disponibilité**	**Les postes de travail sont importants pour effectuer les activités quotidiennes, y compris la correspondance avec les clients, les informations client concernant les affaires, et les informations comptables de base concernant les factures et les créances.**

Tableau 16: Justifications des prescriptions de sécurité

Phase 3 – Sélectionner les cartes de contrôles

Au cours de la phase 3, les membres de l'équipe d'analyse sont en mesure d'«extraire» les cartes de contrôles liées aux domaines de risque applicables déjà définis (lors de la phase 1) et la liste des actifs critiques identifiés. Comme l'indique la figure 5, cette phase comprend trois étapes:

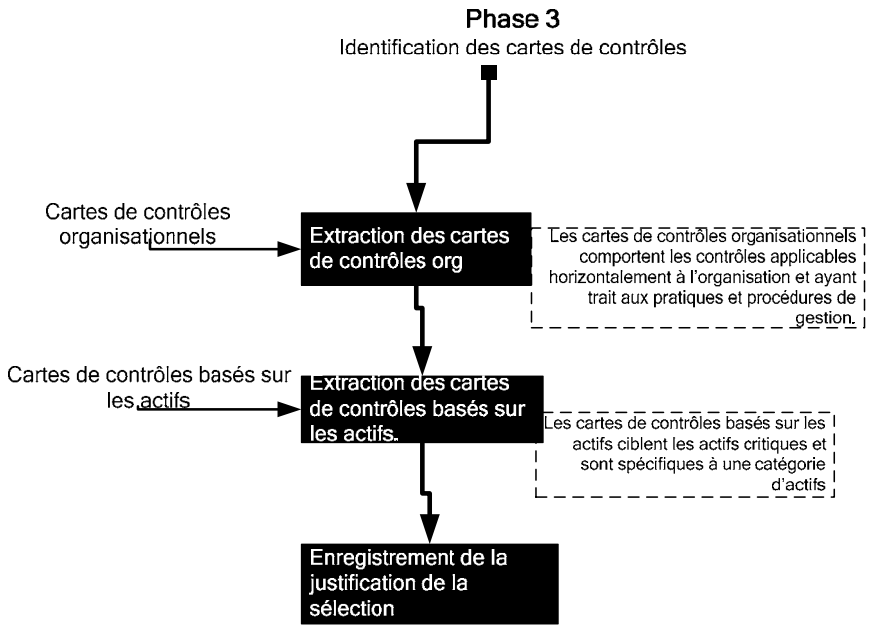

Figure 5: Phase 3 – Processus de sélection des cartes de contrôles

Les cartes de contrôles contiennent les contrôles issus du catalogue de pratiques utilisé dans l'approche OCTAVE. Le catalogue de pratiques regroupe des bonnes pratiques stratégiques et opérationnelles en matière de sécurité. Une organisation qui mène une évaluation des risques liés à la sécurité de l'information s'évalue par rapport à ce catalogue de pratiques. Le catalogue sert à mesurer ce que l'organisation fait correctement actuellement en matière de sécurité (ses pratiques actuelles en matière de sécurité) et ce qu'elle ne fait pas correctement (ses éléments organisationnels vulnérables).

Le catalogue de pratiques est divisé en **deux types de contrôles: les contrôles organisationnels et les contrôles basés sur les actifs:**

- **les contrôles organisationnels** concernent les questions d'organisation au niveau politique et proposent des bonnes pratiques générales en matière de gestion. Les contrôles organisationnels englobent les questions liées à l'activité ainsi que celles nécessitant une planification et une participation de toute l'organisation;
- les pratiques de **contrôles basés sur les actifs** ciblent les problèmes liés à la technologie. Il s'agit des questions afférentes à la façon dont les personnes utilisent la technologie, leur interaction avec celle-ci et la façon dont ils la protègent.

Le catalogue de pratiques est un catalogue général; il n'est pas spécifique à un domaine, à une organisation ou à un règlement. Il peut être modifié pour répondre à une norme de diligence particulière dans un domaine ou à une série de règlements (par exemple, la communauté médicale et les spécifications en matière de sécurité de la loi américaine sur la transférabilité et la responsabilité des assurances de santé (HIPAA)). Il peut également être étendu pour englober des normes spécifiques à l'organisation ou être modifié pour illustrer la terminologie d'un domaine spécifique. **Par ailleurs, il peut être remplacé par toute liste de contrôles standard compatible.**

Les contrôles sont ensuite regroupés en cartes de contrôles distinctes pour deux catégories/ domaines de contrôles: les domaines de contrôles organisationnels et les domaines de contrôles basés sur les actifs. Deux types de cartes de contrôles sont à la disposition des équipes qui analysent une PME:

- **les cartes de contrôles organisationnels** qui comportent les contrôles applicables horizontalement à l'organisation et ayant trait aux pratiques et procédures de gestion. Les cartes de contrôles organisationnels de la sécurité sont généralement vastes et destinées à réduire les risques classiques d'information en fonction du profil organisationnel.
- **les cartes de contrôles basés sur les actifs** ciblent les actifs critiques et sont spécifiques à une catégorie d'actifs. Les cartes de contrôles sont présélectionnées – les contrôles sont regroupés en fonction des profils de risque et des prescriptions de sécurité des actifs. Comme cela a été dit précédemment, les principaux groupes d'actifs de l'organisation sont les suivants: information, système/réseau, personnel et applications. Les cartes de contrôles basés sur les actifs sont conçues pour les tâches quotidiennes et ciblent les risques spécifiques aux actifs.

Une description détaillée des contrôles organisationnels est présentée à l'Annexe C. Contrôles organisationnels.

Étape 1. Sélectionner les cartes de contrôles organisationnels

Au cours de cette étape, les équipes d'analyse choisissent les contrôles organisationnels pour les domaines de risque identifiés au cours de la phase 1 (définition du profil de risque) et définissent ainsi dans quelle direction les efforts de sécurité d'information seront déployés dans l'organisation. Toutefois, des considérations pratiques peuvent empêcher les PME de mettre en œuvre toutes les initiatives immédiatement après l'évaluation. Les organisations disposeront probablement de fonds limités et de peu de personnel disponible pour mettre en œuvre la stratégie de protection. Après l'évaluation, l'équipe d'analyse classe par ordre de priorité les activités dans le cadre de la stratégie de protection et s'attache ensuite à la mise en œuvre des activités dont la priorité est particulièrement élevée.

Les contrôles organisationnels sont disponibles pour chaque profil de risque tel que défini dans la matrice de définition des profils de risque.

Étape 2. Sélectionner les contrôles basés sur les actifs

À partir du profil de risque et des prescriptions de sécurité des actifs, les équipes d'analyse des PME peuvent utiliser le tableau relatif aux cartes de contrôles des actifs (voir Annexe B. Cartes de contrôles des actifs) afin d'identifier les contrôles des actifs adaptés. Les cartes de contrôles des actifs correspondent à des contrôles essentiels regroupés en trois catégories, conformément au profil de risque de l'organisation, à la catégorie d'actif et aux prescriptions de sécurité. Par exemple, les équipes d'analyse ayant un profil d'organisation à haut risque auront des exigences différentes en termes de risques et de sécurité que celles ayant un profil à risque moyen ou faible. Les cartes de contrôles comprendront également davantage de contrôles pour faire face à une plus vaste gamme de prescriptions en termes de risques et de sécurité.

Étape 3. Consigner la liste des contrôles sélectionnés et leur justification

Lors du choix des cartes de contrôles des actifs critiques de l'étape 2, vous discuterez de nombreuses questions liées à ces contrôles. Lors de cette étape, vous justifierez le choix de chaque carte de contrôles et les actions nécessaires de mise en œuvre. En outre, si vous comprenez les cartes de contrôles, vous serez davantage en mesure de définir des plans d'action au cours de la prochaine étape. Pour chaque carte de contrôles, réfléchissez à votre réponse à la question suivante et consignez-la: quelles ressources et quels changements sont nécessaires pour mettre en œuvre les

contrôles sélectionnés? Discutez des aspects opérationnels de chaque contrôle. Posez-vous les questions suivantes pour chacun.

- Qui devrait le mettre en œuvre?
- Qui devrait en être responsable?
- Qui devrait en bénéficier?
- Comment devrait-il être mis en œuvre?

Ces questions permettent de réfléchir à la façon dont les contrôles devraient être utilisés et pourquoi ils sont importants. Si vous ne pouvez répondre seul à toutes ces questions, vous pouvez demander de l'aide à d'autres personnes au sein de votre organisation. Les informations que vous recueillez en répondant à ces questions seront utiles lors de la phase 4 pour l'élaboration des plans de réduction des risques. Veillez à bien consigner ces informations.

Exemple A. (profil de risque: élevé, actif critique: application)

[Etape 1] Lors de l'étape 1, les équipes d'analyse ont sélectionné, à l'aide du **tableau d'évaluation du profil de risque et du tableau des contrôles organisationnels (Tableau 17),** les cartes de contrôles organisationnels pour les domaines de risque identifiés lors de la phase 1 (définition des profils de risque), définissant ainsi dans quelle direction les efforts de sécurité de l'information doivent être déployés dans l'organisation.

Dans l'exemple A, les contrôles organisationnels pour un niveau de risque réglementaire et juridique élevé mettent en place des pratiques de sécurité (contrôles) qui sont dictées par les contrôles organisationnels **SP1** et **SP4**. Dans le même sens, un risque élevé dans la classe de risque de la productivité implique des contre-mesures et des pratiques liées aux contrôles organisationnels **SP3, SP4, SP5** et **SP6**. Pour un niveau de risque moyen en stabilité financière, SP4 est préconisé et pour un niveau de risque faible en matière de renommée et de perte de confiance des clients, SP4.1 (sous-section des contrôles de SP4) est conseillé.

Domaines de risque	Élevé	Moyen	Faible
Juridique et réglementaire	**(SP1)** **(SP4)**	(SP1) (SP4)	SP1.1
Productivité	**(SP3)** **(SP4)** **(SP6)** **(SP5)**	(SP4) (SP6)	SP4.1
Perte financière	(SP2) (SP1) (SP4)	**(SP4)**	SP4.1
Renommée et perte de confiance des clients	(SP1) (SP5)	(SP4) (SP1)	**SP4.1**

Tableau 17: Sélection des contrôles organisationnels – Exemple A

[Étape 2] Lors de l'étape 2, l'équipe d'analyse sélectionne la ou les cartes de contrôles basés sur les actifs en utilisant le tableau des cartes de contrôles basés sur les actifs. Dans l'exemple A, étant

donné le profil de risque élevé de l'organisation identifié lors de la phase 1 et du type d'actifs critiques identifié lors de l'étape 2, l'équipe choisit la carte 1 pour les applications à profil de risque élevé, à savoir la carte CC-1A.

Tableau des cartes de contrôles			
Actifs critiques	**Cartes de risque élevé**	**Cartes de risque moyen**	**Cartes de risque faible**
Application	**CC-1A**	CC-2A	CC-3A
Système	CC-1S	CC-2S	CC-3S
Réseau	CC-1N	CC-2N	CC-3N
Personnel	CC-1P	CC-2P	CC-3P

Tableau 18: Sélection des contrôles basés sur les actifs – Exemple A

La carte sélectionnée dans l'exemple A (voir Annexe B. Cartes de contrôles des actifs) présente les contrôles nécessaires pour une application fonctionnant dans une organisation ayant un profil de risque élevé. L'équipe identifie les contrôles qui concernent les exigences de sécurité définies lors de la phase 3. Dans cet exemple, ce sont les exigences en termes de confidentialité et de disponibilité qui ont été retenues. Les contrôles des actifs **2.1.3, 2.1.6, 2.4.2, 2.5.1** et **2.6.1** sont sélectionnés.

ID carte de contrôles basés sur les actifs		**CC-1A**								
Profil de risque		**Élevé**								
Catégorie d'actif		**Application**								
Prescriptions de sécurité	**Sécurité physique**	**Gestion des systèmes et des réseaux**	**Outils d'administration des systèmes**	**Surveillance et audit de la sécurité des TI**	**Authentification et autorisation**	**Gestion des éléments vulnérables**	**Cryptage**	**Architecture et conception de la sécurité**	**Gestion des incidents**	**Pratiques générales du personnel**
Confidentialité		**2.1.3**			**2.4.2**	**2.5.1**	**2.6.1**			
Intégrité		**2.1.4**			**2.4.2**	**2.5.1**	**2.6.1**			
Disponibilité		**2.1.6**								

Tableau 19: CC-1A Carte de contrôles basés sur les actifs – Exemple A

[Étape 3] Dans l'étape 3, les équipes d'analyse s'occupent de collecter des données et d'analyser les résultats des étapes 1 et 2. Après avoir établi par écrit les étapes précédentes, les contrôles basés sur les actifs sélectionnés et les contrôles organisationnels sont alors recensés dans le tableau ci-dessous.

Actif	**Contrôle**	**Justification de la sélection**
Contrôles basés sur les actifs	**2.1.3**	Les contrôles relatifs à la gestion des systèmes et des réseaux sont essentiels pour assurer la disponibilité et la confidentialité de l'actif étudié.
	2.1.6	
	2.1.4	L'intégrité de l'application est importante car les informations médicales doivent être précises.

	2.4.2	L'authentification et l'autorisation pour les utilisateurs internes et externes ou les tiers peut garantir un accès contrôlé à l'actif étudié.
	2.5.1	La gestion des éléments vulnérables, y compris l'évaluation régulière des éléments vulnérables et les activités nécessaires de restauration, est essentielle afin d'évaluer les mesures et les systèmes de sécurité.
	2.6.1	Les informations confidentielles doivent être protégées pendant leur transport et leur stockage.
Contrôles organisationnels	**SP1**	Sensibilisation et formation à la sécurité
	SP3	Gestion de la sécurité
	SP4	Politique de sécurité
	SP5.	Gestion collaborative
	SP6	Plan anti-sinistre

Tableau 20: Tableau et justification des contrôles sélectionnés– Exemple A

Exemple B. (profil de risque: moyen, actif critique: système)

Lors de l'étape 1, les équipes d'analyse choisissent à l'aide du **tableau des contrôles organisationnels** (Tableau 21) les cartes de contrôles organisationnels pour les domaines de risque identifiés lors de la phase 1 (Étape 1 **- Tableau d'évaluation du profil de risque**), définissant ainsi dans quelle direction les efforts de sécurité de l'information doivent être déployés dans l'organisation.

Dans l'**exemple B**, le contrôle organisationnel prescrit pour un niveau de risque juridique et réglementaire faible est SP1.1 alors que pour un risque faible de productivité et de stabilité financière, le contrôle sera SP4.1. Un niveau de risque moyen de renommée et de perte de confiance des clients exige l'utilisation des contrôles organisationnels SP1 et SP4.

Le Tableau 21 résume la cartographie des contrôles pour l'exemple B susmentionné.

Domaines de risque	**Élevé**	**Moyen**	**Faible.**
Juridique et réglementaire	(SP1)	(SP1)	**SP1.1**
	(SP4)	(SP4)	
Productivité	(SP3)	(SP4)	**SP4.1**
	(SP4)		
	(SP6)	(SP6)	
	(SP5)		
Perte financière	(SP2)	(SP4)	**SP4.1**
	(SP1)		
	(SP4)		
Renommée et perte de confiance des clients	(SP1)	**(SP4)**	SP4.1
	(SP5)	**(SP1)**	

Tableau 21: Sélection des contrôles organisationnels– Exemple B

[Étape 2] Lors de l'étape 2, l'étape d'analyse sélectionne la ou les cartes de contrôles basés sur les actifs en utilisant le tableau des contrôles basés sur les actifs. Dans l'exemple B, étant donné le profil de risque moyen de l'organisation identifié lors de la phase 1 (étape 1) et du type d'actifs critiques identifié lors de l'étape 2, l'équipe choisit la carte 2 pour les systèmes à profil de risque moyen, à savoir la carte CC-2S.

Tableau des cartes de contrôles			
Actifs critiques	**Cartes de risque élevé**	**Cartes de risque moyen**	**Cartes de risque faible**
Application	CC-1A	CC-2A	CC-3A
Système	CC-1S	**CC-2S**	CC-3S
Réseau	CC-1N	CC-2N	CC-3N
Personnel	CC-1P	CC-2P	CC-3P

Tableau 22: Sélection des cartes de contrôles basés sur les actifs– Exemple B

La carte sélectionnée dans l'exemple B (voir Annexe B. Cartes de contrôles des actifs) présente les contrôles nécessaires pour les actifs du système dans une organisation ayant un profil de risque moyen. L'équipe identifie les contrôles qui concernent les prescriptions de sécurité définies lors de la phase 3. D'après les résultats de la phase 2 de l'exemple B (étape 3), les exigences en termes de disponibilité sont utilisées pour identifier les contrôles appropriés à partir de la **carte CC-2S**. Les contrôles des actifs **2.1.7 et 2.1.6** sont donc sélectionnés.

ID carte de contrôles basés sur les actifs										**CC-2S**
Profil de risque										**Moyen**
Catégorie d'actif										**Système**
Prescriptions de sécurité	**Sécurité physique**	**Gestion des systèmes et des réseaux**	**Outils d'administration des systèmes**	**Suivi et audit de la sécurité des TI**	**Authentification et autorisation**	**Gestion des éléments vulnérables**	**Cryptage**	**Architecture et conception de la sécurité**	**Gestion des incidents**	**Pratiques générales du personnel**
Confidentialité		**2.1.6** **2.1.7**			**2.4.1**					
Intégrité		**2.1.9**			**2.4.1**					
Disponibilité		**2.1.6** **2.1.7**								

Tableau 23: CC-2S Carte de contrôles basés sur les actifs – Exemple B

[Étape 3] Dans l'étape 3, les équipes d'analyse s'occupent de collecter des données et d'analyser les résultats des étapes 1 et 2. Après avoir établi par écrit les étapes précédentes, les contrôles basés sur les actifs sélectionnés et les contrôles organisationnels sont alors recensés dans le tableau ci-dessous.

Actif	Contrôle	Justification de la sélection
Contrôles basés sur les actifs	**2.1.6**	Les contrôles relatifs à la gestion des systèmes et des réseaux sont essentiels pour assurer la disponibilité et la confidentialité de l'actif étudié.
	2.1.7	
Contrôles organisationnels	**SP1**	Sensibilisation et formation à la sécurité
	SP4	Politique de sécurité
	SP1.1	Compris dans SP1
	SP4.1	Compris dans SP4

Tableau 24: Justification de la sélection des contrôles– Exemple B

Phase 4 – Gérer et mettre en œuvre

Au cours de la phase 4, l'équipe d'analyse identifie les actions et recommande une liste d'actions, ce qui permet d'orienter l'amélioration de la sécurité. Une bonne mise en œuvre passe impérativement par le soutien des hauts dirigeants (décideurs) à l'égard de l'amélioration continue de la sécurité.

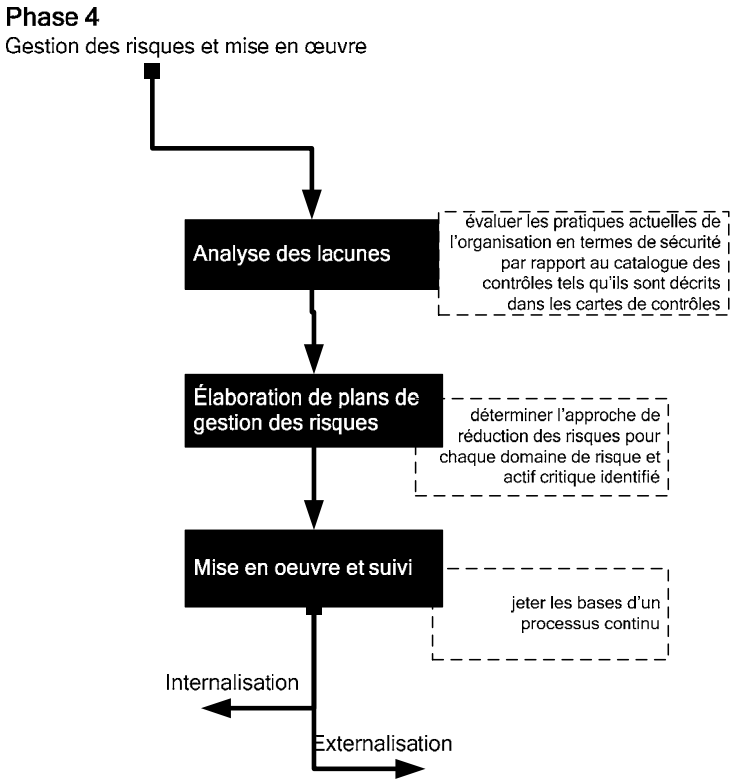

Figure 6: Phase 4 – Processus de mise en œuvre et de gestion

Étape 1. Analyse des lacunes

L'analyse des lacunes est essentielle pour améliorer la façon dont une organisation traite la sécurité de l'information et pour faire un état des lieux de la sécurité, à savoir, ce qui est fait correctement actuellement et les améliorations nécessaires.

Dans cette étape, les équipes d'analyse s'occupent de l'évaluation des pratiques de l'organisation en matière de sécurité par rapport aux contrôles décrits dans les cartes de contrôles. Les équipes d'analyse lisent attentivement les cartes de contrôles choisies et en tirent des informations détaillées sur les politiques, procédures et pratiques actuelles de l'organisation en matière de sécurité, établissant ainsi un point de départ pour le processus d'amélioration.

Au cours du processus d'analyse des lacunes, les équipes utilisent les cartes de contrôles comme des «exigences» et évaluent les lacunes entre ces exigences et les pratiques de sécurité en vigueur tant au niveau organisationnel que des actifs critiques. Les équipes d'analyse doivent consigner minutieusement les résultats sur deux plans – **(1) un pour l'amélioration organisationnelle** et **(2) un pour la protection des actifs**.

Le résultat de ce processus peut servir de base à l'activité de planification qui vient ensuite. Elle comprend deux catégories: (**a) les contrôles organisationnels**, où les équipes d'analyse identifient ce qu'elles font ou ne font pas et définissent des actions pour l'amélioration au niveau organisationnel et **(b) les contrôles basés sur les actifs** où les équipes d'analyse évaluent les mesures de protection existantes pour les actifs critiques identifiés.

Étape 2. Élaboration de plans de réduction des risques

Dans cette étape, les membres de l'équipe d'analyse ont déjà identifié les actifs critiques, le profil de risque de leur organisation, les prescriptions de sécurité, ils ont aussi sélectionné les contrôles appropriés et sont en mesure de définir une approche de réduction des risques pour chaque domaine de risque et actif critique identifié.

Ces premières mesures d'amélioration permettent aux organisations de donner l'élan nécessaire pour mettre en œuvre la stratégie de protection.

Cette activité donne lieu à un plan de réduction des risques, qui **comporte une série de mesures** qu'une organisation peut prendre pour accroître ou conserver son niveau de sécurité existant. Son objectif est d'orienter les futurs efforts en matière de sécurité de l'information au lieu de trouver une solution immédiate à chaque vulnérabilité et problème de sécurité. Étant donné que le plan de réduction des risques donne le cap des activités de sécurité de l'information au niveau de l'organisation, nous suggérons de le structurer autour des cartes de contrôles (organisationnels et basés sur les actifs critiques) sélectionnées (phase 3).

Étape 3. Mise en œuvre, surveillance et contrôle

L'un des principes de la méthode d'évaluation des risques est de jeter les bases d'un processus continu. Dans ce cadre, il est nécessaire de mettre en œuvre les résultats d'une évaluation des risques en matière de sécurité de l'information, afin de jeter les bases de l'amélioration de la sécurité. **Si une organisation ne parvient pas à mettre en œuvre les résultats d'une évaluation, elle ne pourra pas non plus améliorer son dispositif de sécurité.**

L'une des tâches les plus difficiles dans le cadre de l'amélioration est de conserver la dynamique créée au cours de l'évaluation. Toutefois, des considérations pratiques empêcheront beaucoup d'organisations de mettre en œuvre toutes les initiatives immédiatement après l'évaluation. Les PME auront probablement peu de ressources financières et humaines disponibles pour mettre en œuvre la stratégie de protection.

Lors de **cette étape, les équipes d'analyse classent les activités par ordre de priorité puis s'attachent à mettre en œuvre les activités dont la priorité est la plus élevée.**

Trois options sont prévues:

- **Acceptation des risques.** Lorsqu'un risque est accepté, aucune action pour réduire le risque n'est prise et les conséquences si le risque venait à se concrétiser sont acceptées.
- **Réduction des risques**. Lorsqu'un risque est réduit, les actions destinées à maîtriser le danger et ainsi à réduire le risque sont identifiées et appliquées.

À présent que des actions spécifiques ont été identifiées, les membres de l'équipe d'analyse doivent affecter les responsabilités pour les réaliser et fixer une date de réalisation. Les réponses aux questions suivantes doivent être établies par écrit – pour chaque action:

- Qui sera **responsable** de chaque action?
- Que peut faire la direction pour **faciliter** la réalisation de cette action?
- Combien cela **coûtera**-t-il?
- **Combien de temps** cela prendra-t-il?
- **Pouvons-nous le faire nous-mêmes?**
- **Avons-nous besoin d'une aide extérieure?**

NOTE:

Les deux dernières questions sont essentielles pour savoir **si une organisation peut assurer la mise en œuvre** des **contrôles nécessaires en interne.** Les réponses à ces questions sont

également importantes et les décisions sont très difficiles à prendre étant donné que les deux options (externalisation et internalisation) présentent toutes deux des avantages et des inconvénients.

L'externalisation est la **décision de fabriquer ou d'acheter, appliquée à la ressource en question**. Si cela est bien fait, l'externalisation peut présenter des avantages concrets. Les principaux objectifs de l'externalisation sont, outre les fonctions de support, la compression des coûts, la restructuration et une volonté de se recentrer (compétences clés). Le manque de compétences informatiques dans l'organisation peut également motiver l'externalisation des TI. Du fait que les TI acquièrent une importance croissante, les entreprises sont souvent confrontées à une grande disparité entre les capacités et les compétences nécessaires pour réaliser le potentiel des technologies de l'information et la réalité de leur expertise technologique interne.

Toutefois, plusieurs options doivent être envisagées, avec une combinaison de compétences clés de l'organisation et de soutien externe ou de tiers (externalisation complète ou partielle). Comme le montre la figure 7, la gestion et la mise en œuvre peuvent toutes deux être externalisées. **Les offres de services généralement proposées peuvent être résumées comme suit:**

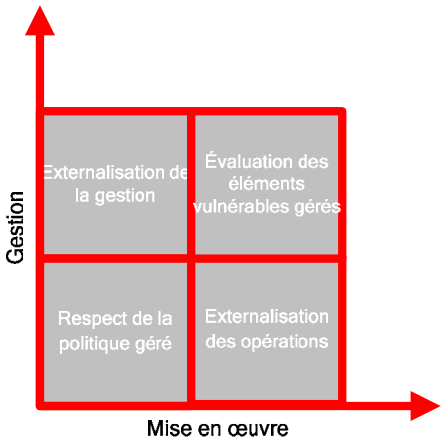

Figure 7: Options d'externalisation de la gestion par rapport à la mise en œuvre

- **Externalisation de la gestion.** En matière d'externalisation de la gestion, les fournisseurs en matière d'externalisation de la gestion proposent des services de gestion de la sécurité de l'information. En d'autres termes, **un responsable de la sécurité est affecté par le fournisseur** pour gérer votre programme de sécurité. Les charges sont généralement calculées sur une base trimestrielle en fonction de la taille et de la complexité de l'organisation, des compétences et de la culture nécessaires.
- **Respect de la politique géré**. Dans les accords de type respect de la politique géré, les conseillers experts en sécurité **mènent régulièrement des audits programmés** afin de garantir le respect permanent de la politique de sécurité de l'information et des contrôles que vous avez mis en place et pour identifier d'éventuelles non conformités. À l'issue de ce processus régulier, vous recevez un rapport détaillé sur l'état global des systèmes, sur les domaines de non-conformité, ainsi que des recommandations sur les mesures à prendre pour que vos systèmes redeviennent conformes. Des rapports et analyses sur les tendances sont généralement prévus afin de vous aider à déterminer si votre situation en matière de sécurité s'améliore ou non et pourquoi.
- **Évaluations des éléments vulnérables gérés.** Dans le cadre de ces formes d'accords de niveaux de services, **les prestataires assurent un éventail unique de services d'évaluation des éléments vulnérables** qui peut être personnalisé en fonction des points d'entrée possibles de l'information de toute organisation – l'internet, les réseaux internes, les applications, l'accès à distance et les installations sans fil. En fonction des moteurs de l'activité, des actifs techniques et des facteurs de risques, les prestataires aident les clients à

déterminer l'intervalle idéal entre chaque évaluation et à définir de façon optimale les limites de l'évaluation.

- **Soutien des opérations géré**. Les services permanents de soutien des opérations fournissent des ressources aux organisations du client afin de couvrir ses **opérations de sécurité interne** au quotidien. Les prestataires proposent généralement des niveaux de soutien différents et modulaires allant du simple conseil/ coaching pour mettre en œuvre les solutions et les politiques de sécurité à l'ingénierie et la mise en œuvre technique de l'infrastructure de sécurité. Les opérations permanentes de sécurité comprennent généralement des tâches telles que le renforcement des serveurs, les modifications de la configuration de sécurité, l'installation de correctifs de la sécurité des applications, etc.
- **Réponse en cas d'urgence et d'incident.** Les services de réponse en cas d'urgence et d'incident assurent une assistance d'ingénieurs experts dans vos locaux dans les situations d'urgence ou de crise. Les services de gestion des incidents et de réponses permettent aux organisations clientes de **répondre rapidement et sûrement aux incidents de sécurité liés à l'informatique** – y compris en cas de compromission de système, infection par un virus et attaques par saturation – en vous aidant à limiter les temps d'arrêt et les pertes de revenus.

Les prescriptions de sécurité des organisations qui externalisent la gestion et le contrôle de l'ensemble ou d'une partie de leurs systèmes, réseaux d'information et/ou environnements informatiques devraient être abordées dans le cadre d'un accord de niveau de service entre les parties. Les questions suivantes (contrôles) devraient au minimum être traitées dans un accord de niveau de service pour l'externalisation de la gestion et des opérations de sécurité de l'information:

A. Niveau d'externalisation et questions de responsabilité
B. Surveillance de la conformité
C. Responsabilités de gestion
D. Étendue des travaux
E. Comment les exigences légales seront-elles respectées, par exemple, la législation sur la protection des données?
F. Quelles seront les dispositions prises pour garantir que toutes les parties prenantes à l'externalisation, dont les sous-traitants, sont informées de leurs responsabilités en termes de sécurité?
G. Comment l'intégrité et la confidentialité des actifs commerciaux de l'organisation seront-elles assurées et testées?
H. Quels seront les contrôles physiques et logiques utilisés pour limiter l'accès aux informations sensibles de l'organisation aux utilisateurs autorisés?
I. Comment la disponibilité des services doit-elle être assurée en cas de catastrophe?
J. Droit d'auditer
K. Ressources, compétences et certificat professionnel
L. Rapport sur le contenu, la fréquence et la structure

Exemple A. (profil de risque: élevé, actif critique: application)

[Étape 1] Lors de cette étape, les équipes d'analyse s'occupent de l'évaluation des pratiques de sécurité en vigueur dans l'organisation par rapport aux contrôles décrits dans les cartes de contrôles. Les équipes d'analyse lisent attentivement les contrôles qui s'appliquent à leur profil (comme l'indiquent les cartes de contrôles sélectionnées - phase 3, étape 3) et en tirent des informations détaillées sur les politiques, procédures et pratiques en matière de sécurité en vigueur dans l'organisation, fournissant ainsi une bonne base d'amélioration.

Le tableau suivant se réfère à l'exemple A:

Actif	Contrôle	Suivons-nous actuellement les contrôles figurant dans les cartes de contrôles?
Contrôles basés sur les actifs	**2.1.3**	Non
	2.1.4	Partiellement
	2.1.6	Non
	2.4.2	Partiellement
	2.5.1	Non
	2.6.1	Non
Contrôles organisationnels	**SP1**	Non
	SP3	Non
	SP4	Oui
	SP5	Non
	SP6	Partiellement

Tableau 25: Liste résultant de l'analyse des lacunes – Exemple A

[Étape 2] Dans l'étape 2, les équipes d'analyse lisent les contrôles (annexes A, B, C, D) et décident des actions nécessaires.

Actif	Contrôle	Action
Contrôles basés sur les actifs	**2.1.3**	L'équipe décide de protéger les informations sensibles par des stockages sécurisés tels que des chaînes de conservation bien définies, des sauvegardes stockées hors site, des moyens de stockage amovibles, des procédures pour la mise au rebut des informations sensibles ou de leur support de stockage.
	2.1.4	L'équipe décide de protéger les informations sensibles en vérifiant régulièrement l'intégrité de la base logicielle installée pour l'application.
	2.1.6	L'équipe décide d'élaborer un plan de sauvegarde des données établi par écrit qui est régulièrement mis à jour, est testé périodiquement, implique des sauvegardes régulièrement programmées des logiciels et des données et exige des essais périodiques et la vérification de la capacité de restauration à partir des sauvegardes.
	2.4.2	L'équipe décide d'établir des politiques et des procédures établies par écrit sur l'utilisation des informations pour l'accès individuel et groupé afin de (A) définir les règles d'octroi du niveau d'accès approprié, (B) définir un droit d'accès initial, (C) modifier le droit d'accès, (D) résilier le droit d'accès et (F) revoir et vérifier périodiquement les droits d'accès.
	2.5.1	L'équipe décide de sélectionner des outils d'évaluation des éléments vulnérables, des listes de contrôle et des scénarios, en les actualisant par rapport aux types d'éléments vulnérables et aux méthodes d'attaque connues, en examinant les sources d'information sur les annonces d'éléments vulnérables, les alertes de sécurité et les notifications, en identifiant les composantes de l'infrastructure à évaluer, en programmant des évaluations des éléments vulnérables, en interprétant les résultats et en y répondant, en assurant le stockage et la suppression sécurisés des données sur les éléments vulnérables.
	2.6.1	L'équipe décide de NE PAS mettre en œuvre le cryptage des données transmises. Les données stockées sont protégées en termes de confidentialité grâce à un système de contrôle d'accès.
Contrôles organisationnels	**SP1**	L'équipe décide de lancer une campagne de sensibilisation de base en assurant une formation de tous les juristes sur les risques liés à l'utilisation du courrier électronique, de l'internet, etc.
	SP3	Fonction de gestion de la sécurité à mettre en place. Un responsable de la sécurité sera affecté.
	SP4	L'équipe décide également d'élaborer une politique de sécurité générique définissant les responsabilités et la propriété des informations.
	SP5	Des procédures de gestion collaborative qui concernent les tiers responsables de la maintenance de l'application sont décidées.
	SP6	Plan anti-sinistre à mettre en œuvre et tester régulièrement.

Tableau 26: Liste d'actions – Exemple A

[Étape 3] Dans l'étape 3 de l'exemple A, les équipes d'analyse classent les activités par ordre de priorité puis s'attachent à mettre en œuvre les activités dont la priorité est la plus haute. Elles décident des actions de priorité élevée à mettre en œuvre au cours du trimestre suivant, les actions de priorité moyenne pour les six prochains mois et les actions de priorité faible à mettre en œuvre avant la fin de l'année à venir.

À présent que vous avez identifié les actions spécifiques de la liste d'actions, vous devez affecter les responsabilités pour les réaliser et fixer une date de réalisation. Répondez aux questions suivantes pour chaque action de votre liste et consignez les résultats:

- Qui sera responsable de chaque action?

- Avant quelle date l'action doit-elle être réalisée?
- Que peut faire la direction pour faciliter la réalisation de cette action?
- Combien cela coûtera-t-il?
- Combien de temps cela prendra-t-il?
- Pouvons-nous le faire nous-mêmes?
- Avons-nous besoin d'une aide extérieure?

Le résultat de leur plan est résumé dans le tableau ci-dessous:

Actif	Contrôle	Responsable	Assistance externe requise	Échéance	Priorité
Contrôles basés sur les actifs	**2.1.3**	Salarié A	Non	mm / jj	Élevée
	2.1.4	Salarié A	Oui		Moyenne
	2.1.6	Salarié A	Oui		Élevée
	2.4.2	Salarié A	Oui		Moyenne
	2.5.1	Salarié A	Non		Faible
	2.6.1	Salarié A	Non		Moyenne
Contrôles organisationnels	**SP1**	Salarié B	Non		Faible
	SP3	Salarié B	Non		Moyenne
	SP4	Salarié B	Oui		Moyenne
	SP5,	Salarié B	Non		Élevée
	SP6	Salarié B	Non		Élevée

Tableau 27: Plan de mise en œuvre – Exemple A

Exemple B. (profil de risque: moyen, actif critique: système)

[Étape 1] Lors de cette étape, les équipes d'analyse s'occupent de l'évaluation des pratiques de sécurité en vigueur dans l'organisation par rapport aux contrôles décrits dans les cartes de contrôles. Les équipes d'analyse lisent attentivement les contrôles qui s'appliquent à leur profil (comme l'indiquent les cartes de contrôles sélectionnées - phase 3, étape 3) et en tirent des informations détaillées sur les politiques, procédures et pratiques en matière de sécurité en vigueur dans l'organisation, fournissant ainsi une bonne base d'amélioration.

Le tableau suivant se réfère à l'exemple B:

Actif	Contrôle	Suivons-nous actuellement les contrôles figurant dans les cartes de contrôles?
Contrôles basés sur les actifs	**2.1.6**	Non
	2.1.7	Oui
Contrôles organisationnels	**SP1**	Partiellement
	SP4	Oui
	SP1.1	Non
	SP4.1	Oui

Tableau 28: Liste résultant de l'analyse des lacunes – Exemple B

[Étape 2] Dans l'étape 2, les équipes d'analyse lisent les contrôles (annexes A, B, C, D) et décident des actions nécessaires.

Actif	Contrôle	Actions
Contrôles basés sur les actifs	**2.1.6**	L'équipe décide d'élaborer un plan de sauvegarde des données établi par écrit, qui est régulièrement mis à jour, est testé périodiquement, implique des sauvegardes régulièrement programmées des logiciels et des données et exige des essais périodiques et la vérification de la capacité de restauration à partir des sauvegardes.
	2.1.7	L'équipe décide d'informer et de former tout le personnel afin qu'il comprenne et soit en mesure d'assumer ses responsabilités dans le cadre des plans de sauvegarde.
Contrôles organisationnels	**SP1**	L'équipe décide de lancer une campagne de sensibilisation de base en assurant une formation de tous les juristes sur les risques liés à l'utilisation du courrier électronique, de l'internet, etc.
	SP4	L'équipe décide également d'élaborer une politique de sécurité générique définissant les responsabilités et la propriété des informations
	SP1.1	Compris dans SP1.
	SP4.1	Compris dans SP4.

Tableau 29: Liste d'actions – Exemple B

[Étape 3] Dans l'étape 3 de l'exemple B, les équipes d'analyse classent les activités par ordre de priorité puis s'attachent à mettre en œuvre les activités dont la priorité est la plus haute. Elles décident des actions de priorité élevée à mettre en œuvre au cours du trimestre suivant, des actions de priorité moyenne pour les six prochains mois et des actions de priorité faible à mettre en œuvre avant la fin de l'année à venir.

À présent que vous avez identifié les actions spécifiques de la liste d'actions, vous devez affecter les responsabilités pour les réaliser et fixer une date de réalisation. Répondez aux questions suivantes pour chaque action de votre liste et consignez les résultats:

- Qui sera responsable de chaque action?
- Avant quelle date l'action doit-elle être réalisée?
- Que peut faire la direction pour faciliter la réalisation de cette action?
- Combien cela coûtera-t-il?
- Combien de temps cela prendra-t-il?
- Pouvons-nous le faire nous-mêmes?

- Avons-nous besoin d'une aide extérieure?

Le résultat de leur plan est résumé dans le tableau ci-dessous:

Actif	Contrôle	Responsable	Assistance externe requise	Échéance	Priorité
Contrôles basés sur les actifs	**2.1.6**	Salarié A	Non	mm / jj	Élevée
	2.1.7	Salarié A	Non		Élevée
Contrôles organisationnels	**SP1**	Salarié A	Non		Moyenne
	SP4	Salarié A	Non		Faible
	SP1.1	Salarié A	Non		Faible
	SP4.1	Salarié A	Non		Élevée

Tableau 30: Plan de mise en œuvre – Exemple B

Annexe A. Cartes de contrôles organisationnels

Sensibilisation et formation à la sécurité (SP1)	
SP1	La carte de contrôles sur la sensibilisation et la formation à la sécurité prévoit des contrôles qui exigent que le personnel comprenne son rôle et ses responsabilités en matière de sécurité. Des séances de sensibilisation et de formation à la sécurité ainsi que des rappels réguliers devraient être dispensés à tout le personnel. Les rôles et responsabilités du personnel devraient être clairement établis par écrit et le respect de ces spécifications devrait être vérifié régulièrement.
Stratégie en matière de sécurité (SP2)	
SP2	La carte de contrôles sur la stratégie en matière de sécurité prévoit des contrôles qui exigent que les stratégies commerciales de l'organisation intègrent systématiquement des considérations relatives à la sécurité. De même, les stratégies et les politiques sur la sécurité doivent prendre en compte les stratégies et objectifs commerciaux de l'organisation. Les stratégies, buts et objectifs en matière de sécurité devraient être établis par écrit et systématiquement revus, mis à jour et communiqués à l'organisation.
Gestion de la sécurité (SP3)	
SP3	La carte de contrôles sur la gestion de la sécurité prévoit des contrôles qui exigent qu'un processus de gestion de la sécurité soit mis en œuvre et appliqué. Le processus doit évaluer en permanence les niveaux de sécurité de l'information requis et définir les contrôles appropriés et affichant un bon rapport coût/risque qui devraient être appliqués et établis par écrit.
Politiques et règles de sécurité (SP4)	
SP4	Cette carte de contrôles exige que l'organisation dispose d'un recueil complet des politiques de sécurité de l'information en vigueur établies par écrit qui sont régulièrement révisées et mises à jour.
Gestion collaborative de la sécurité (SP5)	
SP5	La carte de contrôles sur la gestion collaborative de la sécurité prévoit des contrôles de sécurité mettant en application des procédures établies par écrit, surveillées et appliquées pour protéger les informations de l'organisation lors des échanges avec des organisations externes (par exemple, des tiers, des collaborateurs, des sous-traitants ou des partenaires).
Plan d'urgence/ plan anti-sinistre (SP6)	
SP6	La carte de contrôles sur le plan d'urgence/plan anti-sinistre prévoit des contrôles de sécurité visant à garantir la continuité des opérations de l'organisation en cas de sinistre ou d'indisponibilité des informations. Les principaux éléments de cette carte de contrôles sont les suivants: ▫ plans de continuité des activités ou d'opération d'urgence, ▫ plan(s) anti-sinistre et ▫ plan(s) d'urgence afin de faire face aux situations d'urgence.

Annexe B. Cartes de contrôles des actifs[3]

ID carte de contrôles basés sur les actifs					CC-1A					
Profil de risque					Élevé					
Catégorie d'actif					Application					
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité		2.1.3			2.4.2	2.5.1	2.6.1			
Intégrité		2.1.4			2.4.2	2.5.1	2.6.1			
Disponibilité		2.1.6								

Les contrôles de confidentialité basés sur les applications pour un profil de risque organisationnel élevé concernent généralement les prescriptions de sécurité au niveau d'une application, d'un système, d'un réseau et du personnel afin d'assurer le cycle de vie des informations critiques. Les contrôles sont choisis essentiellement pour éviter que les actifs informationnels ne soient divulgués à des entités non autorisées, qu'elles soient externes ou internes à l'environnement de travail.

Les principaux contrôles pour la protection de la confidentialité des actifs critiques sont les suivants:

OP2.4.2 Ce contrôle nécessite des politiques et des procédures établies par écrit sur l'utilisation des informations pour l'accès individuel et groupé afin de (A) définir les règles d'octroi du niveau d'accès approprié, (B) définir un droit d'accès initial, (C) modifier le droit d'accès, (D) résilier le droit d'accès et (F) revoir et vérifier périodiquement les droits d'accès.

OP2.5.1 Ce contrôle nécessite la présence d'un recueil établi par écrit de procédures visant à gérer les éléments vulnérables, y compris en sélectionnant des outils d'évaluation des éléments vulnérables, des listes de contrôle et des scénarios, en les actualisant par rapport aux types d'éléments vulnérables et aux méthodes d'attaque connus, en examinant les sources d'information sur les annonces de vulnérabilité, les alertes de sécurité et les notifications, en identifiant les composantes de l'infrastructure à évaluer, en programmant des évaluations des éléments vulnérables, en interprétant les résultats et en y répondant, en assurant le stockage et la suppression sécurisés des données sur les éléments vulnérables.

OP2.1.3 Ce contrôle nécessite que les informations sensibles soient protégées grâce à un stockage sécurisé tel que des chaînes de conservation bien définies, des sauvegardes stockées hors site, des moyens de stockage amovibles, des procédures pour la mise au rebut des informations sensibles ou de leur support de stockage.

OP2.1.4 Ce contrôle nécessite que l'intégrité des logiciels installés soit régulièrement vérifiée.

OP2.1.6 Ce contrôle nécessite qu'il existe un plan de sauvegarde des données établi par écrit, régulièrement mis à jour et testé périodiquement, implique des sauvegardes régulièrement programmées des logiciels et des données et exige des essais périodiques et la vérification de la capacité de restauration à partir des sauvegardes.

OP2.6.1 Ce contrôle nécessite que des contrôles de sécurité appropriés soient effectués pour protéger les informations sensibles pendant le stockage et au cours de la transmission, y compris le

[3] L'affectation des contrôles aux cartes de contrôles des actifs dans le cadre de la présente annexe a été réalisée dans la perspective d'établir un degré de protection important. En cas d'actifs comportant des exigences de sécurité très élevées, des contrôles supplémentaires peuvent être envisagés. Toutefois, l'utilisation de ces cartes de contrôles des actifs permet d'obtenir une bonne protection moyenne qui semble appropriée pour la majorité des PME. À moyen terme, l'ENISA prévoit de valider les hypothèses émises dans le présent document grâce à des projets pilotes.

cryptage des données pendant la transmission, le cryptage des données lors de l'écriture sur le disque, l'utilisation d'une infrastructure à clé publique, la technologie relative au réseau privé virtuel et le cryptage de toutes les transmissions basées sur l'internet.

ID carte de contrôles basés sur les actifs					CC-1S					
Profil de risque					Élevé					
Catégorie d'actif					Système					
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Intégrité		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Disponibilité		2.1.6 2.1.7 2.1.9			2.4.6					

Un profil de risque élevé implique des menaces au niveau de l'indisponibilité du système conduisant à l'indisponibilité des services de l'organisation. Les systèmes ne peuvent héberger les applications professionnelles ou peuvent entraîner la perte d'informations critiques. L'origine de ce danger peut être l'instabilité du système due à un dysfonctionnement mécanique ou à une mauvaise installation et utilisation.

Les contrôles de confidentialité basés sur le système destinés à des profils de risque organisationnel élevé impliquent des méthodes garantissant une bonne configuration et une bonne fonctionnalité du système. Les contrôles d'intégrité basés sur le système destiné à un profil de risque organisationnel élevé concernent généralement les prescriptions de sécurité au niveau d'une application, d'un système, d'un réseau et du personnel afin d'assurer la stabilité du système et l'intégrité des informations critiques. La disponibilité constante du système est une condition préalable à la continuité des activités. Les contrôles sont choisis essentiellement pour éviter que les actifs informationnels soient divulgués à des entités non autorisées, qu'elles soient externes ou internes à l'environnement de travail.

Les principaux contrôles pour la protection de l'intégrité des actifs critiques sont les suivants:

OP2.1.3 Ce contrôle nécessite que les informations sensibles soient protégées grâce à un stockage sécurisé tel que des chaînes de conservation bien définies, des sauvegardes stockées hors site, des moyens de stockage amovibles, des procédures pour la mise au rebut des informations sensibles ou de leur support de stockage.

OP2.1.4 Ce contrôle nécessite que l'intégrité des logiciels installés soit régulièrement vérifiée.

OP2.1.5 Ce contrôle nécessite que tous les systèmes soient à jour eu égard aux révisions, correctifs, recommandations relatives aux avis de sécurité.

OP2.1.6 Ce contrôle nécessite qu'il existe un plan de sauvegarde des données établi par écrit qui est régulièrement mis à jour, est testé périodiquement, implique des sauvegardes régulièrement programmées des logiciels et des données et exige des essais périodiques et la vérification de la capacité de restauration à partir des sauvegardes.

OP 2.1.7 Ce contrôle nécessite que tout le personnel comprenne ses responsabilités et soit en mesure de les assumer dans le cadre des plans de sauvegarde.

OP2.1.8 Ce contrôle nécessite que des modifications des matériels et logiciels soient planifiées, contrôlées et établies par écrit.

OP2.1.9 Ce contrôle nécessite que le personnel des TI suive des procédures lors de la création, la modification et la suppression des mots de passe, comptes et privilèges utilisateurs. Une identification unique par utilisateur est nécessaire pour tous les utilisateurs des systèmes d'information, y compris les utilisateurs tiers. Les comptes par défaut et les mots de passe par défaut ont été supprimés des systèmes.

OP2.1.10 Ce contrôle nécessite que seuls les services nécessaires soient exploités sur les systèmes – tous les services superflus doivent être supprimés.

OP2.2.1 Ce contrôle nécessite que les nouveaux outils, procédures et mécanismes de sécurité soient systématiquement revus quant à leur applicabilité pour respecter la stratégie de sécurité de l'organisation.

OP2.2.2 Ce contrôle nécessite que des outils et mécanismes soient utilisés pour l'administration sécurisée des systèmes et des réseaux et soient systématiquement revus et mis à jour ou remplacés. Par exemple: les contrôles d'intégrité des données, les outils cryptographiques, les scanners de vulnérabilité, les outils de vérification de la qualité des mots de passe, les programmes de détection de virus, les outils de gestion de processus, les systèmes de détection d'intrusion, les administrations sécurisées à distance, les outils de service réseau, les analyseurs de trafic, les outils de réponse en cas d'incident, les outils d'analyse judiciaire des données.

OP2.3.1 Ce contrôle nécessite que des outils de surveillance et d'audit des systèmes et des réseaux soient systématiquement utilisés par l'organisation. L'activité est contrôlée par le personnel des TI, l'activité des systèmes et des réseaux est établie par écrit/enregistrée, les journaux sont révisés de façon régulière, les activités inhabituelles sont traitées conformément aux règles ou procédures appropriées, les outils sont révisés et mis à jour régulièrement.

OP2.4.1 Ce contrôle nécessite que des contrôles d'accès et une authentification utilisateur appropriés (par exemple, permissions fichier, configuration réseau) conformes à la politique soient appliqués pour limiter l'accès des utilisateurs à l'information, aux utilitaires, au code source des programmes, aux systèmes sensibles, aux applications et services spécifiques, aux connexions réseau au sein de l'organisation, aux connexions réseau extérieures à l'organisation.

OP2.4.3 Ce contrôle nécessite que les méthodes/mécanismes de contrôle d'accès limitent l'accès aux ressources conformément aux droits d'accès définis par les politiques et procédures.

OP2.4.6 Ce contrôle nécessite que des mécanismes d'authentification soient utilisés pour protéger la disponibilité, l'intégrité et la confidentialité des informations sensibles. Par exemple avec des signatures numériques et la biométrie.

OP2.6.1 Ce contrôle nécessite que des contrôles de sécurité appropriés soient effectués pour protéger les informations sensibles pendant le stockage et au cours de la transmission, y compris le cryptage des données pendant la transmission, le cryptage des données lors de l'écriture sur le disque, l'utilisation d'une infrastructure à clé publique, la technologie relative au réseau privé virtuel, et le cryptage de toutes les transmissions basées sur l'internet.

OP2.7.1 Ce contrôle nécessite que l'architecture et la conception des systèmes pour les systèmes nouveaux et révisés intègrent des considérations en matière de stratégies, politiques et procédures de sécurité, l'historique des compromissions de sécurité et les résultats des évaluations des risques en matière de sécurité.

OP2.7.2 Ce contrôle nécessite que l'organisation dispose de diagrammes actualisés qui présentent l'architecture de sécurité de toute l'entreprise et la topologie du réseau.

ID carte de contrôles basés sur les actifs					CC-1N					
Profil de risque					Élevé					
Catégorie d'actif					Réseau					
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du
Confidentialité					2.4.6	2.5.3	2.6.1			
Intégrité	1.1.4	2.1.1 2.1.10			2.4.1 2.4.3 2.4.4 2.4.6	2.5.3		2.7.2		
Disponibilité	1.1.4				2.4.6					

Un profil de risque élevé implique des menaces au niveau des éléments vulnérables du réseau qui peuvent conduire à des attaques externes ou un accès interne non autorisé à certains domaines du réseau présentant un intérêt ou un risque élevé.

Les lacunes en matière de sécurité du réseau ont des conséquences immédiates et directes sur les applications exécutées et les flux d'informations.

Les contrôles de confidentialité basés sur le réseau pour un profil de risque organisationnel élevé devraient protéger les informations critiques et internes d'une éventuelle perte ou mauvaise utilisation. Par ailleurs, les informations stockées dans les réseaux doivent être disponibles et facilement accessibles et dissociées en fonction de leur degré de criticité.

Les contrôles essentiels pour préserver la confidentialité, l'intégrité et la disponibilité au sein d'un réseau sont les suivants:

OP2.6.1 Ce contrôle nécessite que des contrôles de sécurité appropriés soient effectués pour protéger les informations sensibles pendant le stockage et au cours de la transmission, y compris le cryptage des données pendant la transmission, le cryptage des données lors de l'écriture sur le disque, l'utilisation d'une infrastructure à clé publique, la technologie relative au réseau privé virtuel et le cryptage de toutes les transmissions basées sur l'internet.

OP2.4.6 Ce contrôle nécessite que des mécanismes d'authentification soient utilisés pour protéger la disponibilité, l'intégrité et la confidentialité des informations sensibles. Par exemple avec des signatures numériques et la biométrie.

OP2.7.2 Ce contrôle nécessite que l'organisation dispose de diagrammes actualisés qui présentent l'architecture de sécurité de toute l'entreprise et la topologie du réseau.

OP2.1.1 Ce contrôle nécessite un ou plusieurs plans de sécurité établis par écrit pour la protection des systèmes et des réseaux.

OP2.4.1 Ce contrôle nécessite que des contrôles d'accès et une authentification utilisateur appropriés (par exemple, permissions fichier, configuration réseau) conformes à la politiques soient appliqués pour limiter l'accès des utilisateurs à l'information, aux utilitaires, au code source des programmes, aux systèmes sensibles, aux applications et services spécifiques, aux connexions réseau au sein de l'organisation, aux connexions réseau extérieures à l'organisation.

OP2.4.3 Ce contrôle nécessite que les méthodes/mécanismes de contrôle d'accès limitent l'accès aux ressources conformément aux droits d'accès définis par les politiques et procédures.

OP2.1.10 Ce contrôle nécessite que seuls les services nécessaires soient exploités sur les systèmes – tous les services superflus doivent être supprimés.

OP 2.5.3 Ce contrôle nécessite que des évaluations des éléments vulnérables de la technologie soient menées de façon périodique et que les éléments vulnérables soient traités dès qu'ils sont identifiés.

OP1.1.4 Ce contrôle nécessite la présence de politiques et procédures établies par écrit pour la gestion des visiteurs, y compris, ouverture de session, personnel d'escorte, registres des accès, réception et hébergement.

OP2.4.6 Ce contrôle nécessite que des mécanismes d'authentification soient utilisés pour protéger la disponibilité, l'intégrité et la confidentialité des informations sensibles. Par exemple avec des signatures numériques et la biométrie.

ID carte de contrôles basés sur les actifs										CC-1P
Profil de risque										Élevé
Catégorie d'actif										Personnel
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité										3.2.1 3.2.2 3.2.3
Intégrité	1.1.4 1.3.2									3.2.1 3.2.2 3.2.3
Disponibilité										

Un profil de risque élevé implique des menaces au niveau de la gestion du personnel et des ressources humaines en général. Le degré d'engagement du personnel dans l'utilisation des contrôles de sécurité appropriés sur les ressources du réseau détermine le niveau de protection qui peut être obtenu.

La manipulation d'informations et la réutilisation d'anciens registres présentant une grande valeur pour l'organisation est un aspect critique. Les informations internes ou confidentielles du personnel doivent être traitées respectueusement. La surveillance des politiques du personnel sur ces procédures garantit la confidentialité, l'intégrité et la disponibilité de l'information.

Les contrôles essentiels pour garantir la confidentialité, l'intégrité et la disponibilité de l'information en association avec du personnel de type actif critique sont les suivants:

OP3.2.1 Ce contrôle nécessite que les membres du personnel adoptent de bonnes pratiques en matière de sécurité: sécurisation de l'information dont ils sont responsables, pas de divulgation des informations sensibles à autrui (résistance face à l'ingénierie sociale), bonnes capacités pour utiliser les matériels et logiciels des technologies de l'information, application de bonnes pratiques concernant les mots de passe, compréhension et application des politiques et règles de sécurité, identification des incidents et établissement de rapports.

OP3.2.2 Ce contrôle nécessite que tout le personnel à tous les niveaux de responsabilité mette en œuvre les rôles et responsabilités qui lui ont été attribués en matière de sécurité de l'information.

OP3.2.3 Ce contrôle nécessite l'existence de procédures établies par écrit pour l'autorisation et la surveillance du personnel travaillant avec des informations sensibles ou sur des sites où ces informations sont stockées. Il s'agit des salariés, contractants, partenaires, collaborateurs et personnel des organisations tierces, personnel de maintenance des systèmes ou personnel de maintenance des installations.

OP1.1.4 Ce contrôle nécessite la présence de politiques et procédures établies par écrit pour la gestion des visiteurs, y compris, ouverture de session, personnel d'escorte, registres des accès, réception et hébergement.

OP1.3.2 Ce contrôle nécessite que les actions individuelles ou groupées – concernant tous les supports contrôlés physiquement – puissent être justifiées.

ID carte de contrôles basés sur les actifs					CC-2A					
Profil de risque					**Moyen**					
Catégorie d'actif					**Application**					
Prescriptions de sécurité	**Sécurité physique**	**Gestion des systèmes et des réseaux**	**Outils d'administration des systèmes**	**Suivi et audit de la sécurité des TI**	**Authentification et autorisation**	**Gestion des éléments vulnérables**	**Cryptage**	**Architecture et conception de la sécurité**	**Gestion des incidents**	**Pratiques générales du personnel**
Confidentialité					**2.4.2**		**2.6.1**			
Intégrité					**2.4.2**					
Disponibilité		**2.1.6** **2.1.7**								

Un profil de risque moyen implique le stockage et le traitement d'informations faisant l'objet de droits de propriété et présentant généralement un profil de risque générique où des entités externes malveillantes tentent d'entraver ou de compromettre la confidentialité d'informations spécifiques et de valeur moyenne. Les contrôles de confidentialité basés sur les applications pour un profil de risque organisationnel moyen concernent généralement les prescriptions de sécurité au niveau d'une application, un système, un réseau et du personnel afin de protéger le cycle de vie des informations critiques. Les contrôles d'intégrité basés sur les applications pour un profil de risque organisationnel moyen définissent le degré de précision des informations d'une application alors que la disponibilité renvoie au degré d'accessibilité.

Les principaux contrôles pour la protection de la confidentialité, l'intégrité et la disponibilité au niveau des applications sont les suivants:

OP2.4.2 Ce contrôle nécessite la présence de politiques et de procédures établies par écrit sur l'utilisation des informations pour l'accès individuel et groupé afin de définir les règles d'octroi du niveau d'accès approprié, définir un droit d'accès initial, modifier le droit d'accès, résilier le droit d'accès et revoir et vérifier périodiquement les droits d'accès.

OP2.6.1 Ce contrôle nécessite que des contrôles de sécurité appropriés soient effectués pour protéger les informations sensibles pendant le stockage et au cours de la transmission, y compris le cryptage des données pendant la transmission, le cryptage des données lors de l'écriture sur le disque, l'utilisation d'une infrastructure à clé publique, la technologie relative au réseau privé virtuel et le cryptage de toutes les transmissions basées sur l'internet.

OP2.1.6 Ce contrôle nécessite qu'il existe un plan de sauvegarde des données établi par écrit qui est régulièrement mis à jour, est testé périodiquement, implique des sauvegardes régulièrement programmées des logiciels et des données et exige des essais périodiques et la vérification de la capacité de restauration à partir des sauvegardes.

OP2.1.7 Ce contrôle nécessite que tout le personnel comprenne ses responsabilités et soit en mesure de les assumer dans le cadre des plans de sauvegarde.

ID carte de contrôles basés sur les actifs										CC-2S
Profil de risque										Moyen
Catégorie d'actif										Système
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité		2.1.6 2.1.7			2.4.1					
Intégrité		2.1.9			2.4.1					
Disponibilité		2.1.6 2.1.7								

Un profil de risque moyen implique des menaces modérées au niveau des instabilités du système conduisant à l'indisponibilité du service pendant une courte durée. Les systèmes ne peuvent supporter les applications ou fonctionner correctement.

Les contrôles basés sur le système pour des profils de risque organisationnel moyen englobent les méthodes garantissant une bonne configuration et une bonne fonctionnalité du système pour un accès approprié.

Les principaux contrôles pour la protection de la confidentialité, l'intégrité et la disponibilité au sein des systèmes sont les suivants:

OP2.4.1 Ce contrôle nécessite que des contrôles d'accès et une authentification utilisateur appropriés (par exemple, permissions fichier, configuration réseau) conformes à la politiques soient appliqués pour limiter l'accès des utilisateurs à l'information, aux utilitaires, au code source des programmes, aux systèmes sensibles, aux applications et services spécifiques, aux connexions réseau au sein de l'organisation, aux connexions réseau extérieures à l'organisation.

OP2.1.6 Ce contrôle nécessite qu'il existe un plan de sauvegarde des données établi par écrit qui est régulièrement mis à jour, est testé périodiquement, implique des sauvegardes régulièrement programmées des logiciels et des données et exige des essais périodiques et la vérification de la capacité de restauration à partir des sauvegardes.

OP2.1.7 Ce contrôle nécessite que tout le personnel comprenne ses responsabilités et soit en mesure de les assumer dans le cadre des plans de sauvegarde.

OP2.1.9 Ce contrôle nécessite que le personnel des TI suive des procédures lors de la création, la modification et la suppression des mots de passe, comptes et privilèges utilisateurs. Une identification unique par utilisateur est nécessaire pour tous les utilisateurs des systèmes d'information, y compris les utilisateurs tiers. Les comptes par défaut et les mots de passe par défaut ont été supprimés des systèmes.

ID carte de contrôles basés sur les actifs							CC-2N			
Profil de risque							Moyen			
Catégorie d'actif							Réseau			
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables (OP2.5)	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité							2.6.1			
Intégrité					2.4.3					
Disponibilité		2.1.5								

Un profil de risque moyen implique des menaces au niveau des éléments vulnérables du réseau en raison d'une architecture réseau mauvaise ou mal appliquée qui peut conduire à des attaques externes ou un accès interne non autorisé à certains domaines du réseau présentant un intérêt ou une valeur moyenne pour l'organisation.

Les lacunes en matière de sécurité du réseau ont des conséquences immédiates et directes sur les applications exécutées et les flux d'informations. Le risque est jugé moyen lorsque le système ne permet pas l'accès à des composantes critiques qui pourraient affecter la renommée de l'organisation ou sa bonne santé financière.

Les principaux contrôles pour la protection de la confidentialité, l'intégrité et la disponibilité au sein d'un réseau sont les suivants:

OP2.6.1 Ce contrôle nécessite que des contrôles de sécurité appropriés soient effectués pour protéger les informations sensibles pendant le stockage et au cours de la transmission, y compris le cryptage des données pendant la transmission, le cryptage des données lors de l'écriture sur le disque, l'utilisation d'une infrastructure à clé publique, la technologie relative au réseau privé virtuel et le cryptage de toutes les transmissions basées sur l'internet.

OP2.4.3 Ce contrôle nécessite que les méthodes/mécanismes de contrôle d'accès limitent l'accès aux ressources conformément aux droits d'accès définis par les politiques et procédures.

OP2.1.5 Ce contrôle nécessite que tous les systèmes soient à jour eu égard aux révisions, correctifs, recommandations relatives aux avis de sécurité.

ID carte de contrôles basés sur les actifs										CC-2P
Profil de risque										Moyen
Catégorie d'actif										Personnel
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables (OP2.5)	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité										3.2.1 3.2.2
Intégrité										3.2.1 3.2.2
Disponibilité	1.1.4									

Un profil de risque moyen implique des menaces au niveau de la gestion des ressources humaines dans les moyennes entreprises lorsque les pratiques de sécurité en vigueur pourraient engendrer des problèmes ayant un impact modéré.

Les incidents liés à une mauvaise utilisation des mots de passe et des droits d'accès peuvent conduire à des fuites d'informations. Un niveau de confidentialité moyen des informations détermine le niveau de risque ou les pertes financières pour l'organisation.

La surveillance des politiques du personnel sur ces procédures garantit la confidentialité, l'intégrité et la disponibilité de l'information.

Les contrôles essentiels pour garantir la confidentialité, l'intégrité et la disponibilité de l'information en association avec du personnel de type actif critique sont les suivants:

OP3.2.1 Ce contrôle nécessite que les membres du personnel adoptent de bonnes pratiques en matière de sécurité: sécurisation de l'information dont ils sont responsables, pas de divulgation des informations sensibles à autrui (résistance face à l'ingénierie sociale), bonnes capacités pour utiliser les matériels et logiciels des technologies de l'information, application de bonnes pratiques concernant les mots de passe, compréhension et application des politiques et règles de sécurité, identification des incidents et établissement de rapports.

OP3.2.2 Ce contrôle nécessite que tout le personnel à tous les niveaux de responsabilité mette en œuvre les rôles et responsabilités qui lui ont été attribués en matière de sécurité de l'information.

OP1.1.4 Ce contrôle nécessite la présence de politiques et procédures établies par écrit pour la gestion des visiteurs, y compris, ouverture de session, personnel d'escorte, registres des accès, réception et hébergement.

ID carte de contrôles basés sur les actifs					CC-3A					
Profil de risque					Faible					
Catégorie d'actif					Application					
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables (OP2.5)	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité					2.4.2					
Intégrité										
Disponibilité										

Un profil de risque faible implique le stockage et le traitement d'informations publiques ou internes n'ayant pas une importance critique, qui entraînerait des pertes financières minimes. La renommée de l'organisation n'est pas menacée. Toutefois, des contrôles doivent être opérés afin de prévenir ce type de fuites d'informations et de sécuriser le cycle de vie de l'information.

Par ailleurs, même s'il n'y a aucun impact sur la confidentialité, l'intégrité et la disponibilité de l'information doivent être garanties pour tout utilisateur autorisé.

Le contrôle essentiel pour la confidentialité au niveau de l'actif application est le suivant:

OP2.4.2 Ce contrôle nécessite la présence de politiques et de procédures établies par écrit sur l'utilisation des informations pour l'accès individuel et groupé afin de définir les règles d'octroi du niveau d'accès approprié, définir un droit d'accès initial, modifier le droit d'accès, résilier le droit d'accès et revoir et vérifier périodiquement les droits d'accès.

ID carte de contrôles basés sur les actifs					CC-3S					
Profil de risque					Faible					
Catégorie d'actif					Système					
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables (OP2.5)	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité		2.1.9			2.4.1					
Intégrité					2.4.1					
Disponibilité		2.1.6								

Un profil de risque faible implique un niveau de menaces faible en ce qui concerne les instabilités du système, conduisant à l'indisponibilité du service pendant une courte durée.

Les contrôles basés sur le système pour des profils de risque organisationnel minime englobent les méthodes garantissant une bonne configuration et une bonne fonctionnalité du système pour un accès approprié.

L'impact de l'indisponibilité du système n'affecte pas la renommée de l'organisation car les informations ne sont ni privées ni critiques pour l'organisation.

L'indisponibilité du système n'affecte pas la qualité du service ou des produits.

Les principaux contrôles pour la protection de la confidentialité et la disponibilité au sein des systèmes sont les suivants:

OP2.4.1 Ce contrôle nécessite que des contrôles d'accès et une authentification utilisateur appropriés (par exemple, permissions fichier, configuration réseau) conformes à la politiques soient appliqués pour limiter l'accès des utilisateurs à l'information, aux utilitaires, au code source des programmes, aux systèmes sensibles, aux applications et services spécifiques, aux connexions réseau au sein de l'organisation, aux connexions réseau extérieures à l'organisation.

OP2.1.6 Ce contrôle nécessite qu'il existe un plan de sauvegarde des données établi par écrit qui est régulièrement mis à jour, est testé périodiquement, implique des sauvegardes régulièrement programmées des logiciels et des données et exige des essais périodiques et la vérification de la capacité de restauration à partir des sauvegardes.

OP2.1.9 Ce contrôle nécessite que le personnel des TI suive des procédures lors de la création, la modification et la suppression des mots de passe, comptes et privilèges utilisateurs. Une identification unique par utilisateur est nécessaire pour tous les utilisateurs des systèmes d'information, y compris les utilisateurs tiers. Les comptes par défaut et les mots de passe par défaut ont été supprimés des systèmes.

ID carte de contrôles basés sur les actifs							CC-3N			
Profil de risque							Faible			
Catégorie d'actif							Réseau			
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables (OP2.5)	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité							2.6.1			
Intégrité										
Disponibilité										

Un profil de risque faible implique des menaces au niveau des éléments vulnérables mineurs du réseau ou l'indisponibilité des informations en raison d'une architecture réseau déficiente ou mal appliquée. L'impact pourrait toutefois être jugé insignifiant étant donné que les informations présentent peu d'intérêt et qu'elles ne sont pas très confidentielles pour l'organisation. Le risque de perte financière pour l'organisation est donc faible.

Toutefois, des contrôles de sécurité sont recommandés au niveau du cryptage des informations transférées.

Le principal contrôle pour la protection de la confidentialité au sein d'un réseau est le suivant:

OP2.6.1 Ce contrôle nécessite que des contrôles de sécurité appropriés soient effectués pour protéger les informations sensibles pendant le stockage et au cours de la transmission, y compris le cryptage des données pendant la transmission, le cryptage des données lors de l'écriture sur le disque, l'utilisation d'une infrastructure à clé publique, la technologie relative au réseau privé virtuel et le cryptage de toutes les transmissions basées sur l'internet.

ID carte de contrôles basés sur les actifs										CC-3P
Profil de risque										Faible
Catégorie d'actif										Personnel
Prescriptions de sécurité	Sécurité physique	Gestion des systèmes et des réseaux	Outils d'administration des systèmes	Suivi et audit de la sécurité des TI	Authentification et autorisation	Gestion des éléments vulnérables (OP2.5)	Cryptage	Architecture et conception de la sécurité	Gestion des incidents	Pratiques générales du personnel
Confidentialité										
Intégrité										
Disponibilité	1.1.4									

Un profil de risque faible implique des menaces potentielles ayant un faible impact sur la gestion des ressources humaines lorsque les pratiques de sécurité en vigueur pourraient engendrer des problèmes mais présentant un risque minime pour l'organisation.

Le niveau de criticité des informations est peu élevé. Ainsi l'impact financier est faible et les pertes financières peuvent être considérées comme insignifiantes.

Toutefois, la surveillance des politiques du personnel y compris sur ces procédures garantit la confidentialité, l'intégrité et la disponibilité de l'information.

Le principal contrôle pour garantir la confidentialité, l'intégrité et la disponibilité de l'information en relation avec le personnel est le suivant:

OP1.1.4 Ce contrôle nécessite la présence de politiques et procédures établies par écrit pour la gestion des visiteurs, y compris, ouverture de session, personnel d'escorte, registres des accès, réception et hébergement.

Annexe C. Contrôles organisationnels

Sensibilisation et formation à la sécurité (SP1)	
SP1.1	Les membres du personnel comprennent leur rôle et leurs responsabilités en matière de sécurité. Cela est établi par écrit et vérifié.
SP1.2	Il existe une expertise interne suffisante pour tous les services, mécanismes et technologies supportés (par exemple, journalisation, surveillance et cryptage), y compris leur exploitation sécurisée. Cela est établi par écrit et vérifié.
SP1.3	Des séances de sensibilisation, de formation et de rappels réguliers sur la sécurité sont dispensées à l'ensemble du personnel. Les connaissances du personnel sont établies par écrit et leur conformité est vérifiée régulièrement. La formation porte sur les sujets suivants:
	– stratégies, buts et objectifs en matière de sécurité
	– règlementations, règles et procédures de sécurité
	– politiques et procédures de travail avec des tiers
	– plans d'urgence et anti-sinistre
	– prescriptions de sécurité physique
	– perspective des utilisateurs
	– gestion des systèmes et des réseaux
	– outils d'administration des systèmes
	– surveillance et audit concernant la sécurité physique et des technologies de l'information
	– authentification et autorisation
	– gestion des éléments vulnérables
	– cryptage
	– architecture et conception
	– gestion des incidents
	– pratiques générales du personnel
	– application, sanctions et actions disciplinaires pour les atteintes à la sécurité
	– comment accéder correctement aux informations sensibles ou travailler dans les zones où des informations sensibles sont accessibles
	– politiques de licenciement et procédures relatives à la sécurité

Stratégie en matière de sécurité (SP2)	
SP2.1	Les stratégies commerciales de l'organisation intègrent systématiquement des considérations relatives à la sécurité.
SP2.2	Les stratégies et les politiques sur la sécurité prennent en compte les stratégies et objectifs commerciaux de l'organisation.
SP2.3	Les stratégies, buts et objectifs en matière de sécurité sont établis par écrit et systématiquement revus, mis à jour et communiqués à l'organisation.

Gestion de la sécurité (SP3)	
SP3.1	La direction affecte suffisamment de fonds et de ressources aux activités relatives à la sécurité de l'information.
SP3.2	Les rôles et responsabilités en termes de sécurité sont définis pour tout le personnel de l'organisation.
SP3.3	Les pratiques de l'organisation en matière de recrutement et de licenciement du personnel tiennent compte des questions relatives à la sécurité de l'information.
SP3.4	Les niveaux requis de sécurité de l'information et la façon dont ils sont appliqués aux individus et aux groupes sont établis par écrit et appliqués.
SP3.5	L'organisation gère les risques liés à la sécurité de l'information, y compris
	– en évaluant les risques liés à la sécurité de l'information régulièrement mais aussi en réponse à des évolutions majeures de la technologie, des menaces internes/externes ou des systèmes et opérations de l'organisation
	– en prenant des mesures pour réduire les risques à un niveau acceptable
	– en maintenant un niveau de risque acceptable
	– en utilisant des évaluations des risques liés à la sécurité de l'information pour aider à choisir des mesures de contrôle/ de sécurité rentables en appréciant les coûts de mise en œuvre par rapport aux pertes potentielles
SP3.6	La direction reçoit des rapports réguliers, et agit en fonction de ces rapports qui synthétisent les résultats des
	– revues des journaux d'exploitation
	– revues des pistes de vérification
	– évaluations des éléments vulnérables technologiques
	– incidents de sécurité et réponses apportées
	– évaluations des risques
	– revues de sécurité physique
	– plans et recommandations pour l'amélioration de la sécurité

Politiques et règles de sécurité (SP4)	
SP4.1	L'organisation dispose d'un recueil complet des politiques de sécurité de l'information en vigueur établies par écrit qui sont régulièrement révisées et mises à jour. Ces politiques traitent des principaux domaines thématiques de la sécurité, dont:
	– · la stratégie et la gestion de la sécurité
	– · la gestion des risques liés à la sécurité
	– · la sécurité physique
	– · la gestion des systèmes et des réseaux
	– · les outils d'administration des systèmes
	– · la surveillance et les audits
	– · l'authentification et l'autorisation
	– · la gestion des éléments vulnérables
	– · le cryptage
	– · l'architecture et la conception de la sécurité
	– · la gestion des incidents
	– · les pratiques du personnel en matière de sécurité
	– · les lois et règlements applicables
	– · la sensibilisation et la formation
	– · la gestion collaborative de la sécurité de l'information
	– · les plans d'urgence et anti-sinistre
SP4.2	Il existe un processus établi par écrit pour la gestion des politiques en matière de sécurité, comprenant
	– · la création
	– · l'administration (avec des revues et mises à jour régulières)
	– · la communication
SP4.3	L'organisation dispose d'un processus établi par écrit pour l'évaluation régulière (technique et non technique) du respect des politiques de sécurité de l'information, des lois et règlements applicables et des prescriptions d'assurance.
SP4.4	L'organisation dispose d'un processus établi par écrit pour garantir le respect des politiques de sécurité de l'information, des lois et règlements applicables et des prescriptions d'assurance.
SP4.5	L'organisation applique de façon uniforme ses politiques en matière de sécurité.
SP4.6	Les tests et la révision des politiques et procédures de sécurité sont réservés au personnel dûment autorisé.

Gestion collaborative de la sécurité (SP5)	
SP5.1	L'organisation dispose de procédures établies par écrit, surveillées et appliquées pour protéger les informations de l'organisation lors des échanges avec des organisations externes (par exemple, des tiers, des collaborateurs, des sous-traitants ou des partenaires).
SP5.2	L'organisation a vérifié que les services, les mécanismes et les technologies de sécurité externalisés satisfont ses attentes et ses exigences.
SP5.3	L'organisation documente, surveille et applique les stratégies de protection des informations appartenant à des organisations externes, qui sont consultées à partir de ses propres infrastructures ou utilisées par son propre personnel.
SP5.4	L'organisation dispense des séances de sensibilisation et de formation sur les politiques et procédures de sécurité applicables des organisations externes pour le personnel travaillant avec ces organisations et en vérifie les effets.
SP5.5	Il existe des procédures établies par écrit pour le personnel externe licencié spécifiant les mesures de sécurité pertinentes pour supprimer leur accès. Ces procédures sont communiquées et coordonnées avec l'organisation externe.

Plan d'urgence/ plan anti-sinistre (SP6)	
SP6.1	Une analyse de la criticité des opérations, des applications et des données a été réalisée.
SP6.2	L'organisation a établi par écrit
	– · des plans de continuité des activités ou d'opération d'urgence
	– · un ou plusieurs plan(s) anti-sinistre
	– · un ou plusieurs plan(s) d'urgence afin de faire face aux situations d'urgence
SP6.3	Les plans d'urgence, anti-sinistre et de continuité des activités tiennent compte des spécifications et des contrôles en matière d'accès physique et électronique.
SP6.4	Les plans d'urgence, anti-sinistre et de continuité des activités sont régulièrement revus, testés et révisés.
SP6.5	Tout le personnel
	– · a connaissance des plans d'urgence, anti-sinistre et de continuité des activités
	– · les comprend et est en mesure d'assumer ses responsabilités

Annexe D. Contrôles basés sur les actifs

Sécurité physique (OP1)	
Plans et procédures de sécurité physique (OP1.1)	
OP1.1.1	Il existe des plans établis par écrit sur la sécurité des installations pour la protection des locaux, des bâtiments et de toute zone à accès restreint.
OP1.1.2	Ces plans sont régulièrement revus, testés et mis à jour.
OP1.1.3	Les procédures et mécanismes relatifs à la sécurité physique sont systématiquement testés et révisés.
OP1.1.4	Il existe des politiques et des procédures établies par écrit pour gérer les visiteurs, y compris
	– · l'ouverture de session
	– · le personnel d'escorte
	– · les registres des accès
	– · la réception et l'hébergement
OP1.1.5	Il existe des politiques et des procédures établies par écrit pour le contrôle physique du matériel et des logiciels, dont
	– les stations de travail, ordinateurs portables, modems, composants sans fil et autres composants utilisés pour l'accès aux informations
	– l'accès, le stockage et la localisation des sauvegardes de données
	– le stockage des informations sensibles sur des supports physiques et électroniques
	– ·la suppression des informations sensibles ou des supports sur lesquels elles sont stockées
	– la réutilisation et le recyclage des supports papier et électronique
Contrôle d'accès physique (OP1.2)	
OP1.2.1	Il existe des politiques et des procédures établies par écrit pour l'accès des individus ou des groupes, couvrant
	– · les règles pour l'octroi du niveau pertinent d'accès physique
	– · les règles pour l'établissement du droit d'accès initial
	– · la modification du droit d'accès
	– · la résiliation du droit d'accès
	– · la revue et la vérification périodique des droits d'accès
OP1.2.2	Il existe des politiques, des procédures et des mécanismes établis par écrit pour contrôler l'accès physique dans des entités données. Cela comprend:
	– · les domaines de travail
	– · les supports matériels (ordinateurs, appareils de communication, etc.) et logiciels
OP1.2.3	Il existe des procédures établies par écrit pour vérifier l'autorisation d'accès avant d'autoriser l'accès physique.
OP1.2.4	Les postes de travail et autres composants qui permettent l'accès aux informations sensibles sont physiquement protégés de tout accès non autorisé.
Surveillance et audit de la sécurité physique (OP1.3)	
OP1.3.1	Les registres de maintenance sont tenus à jour pour consigner les réparations et les modifications des composantes physiques d'une installation.
OP1.3.2	Les actions individuelles ou groupées, concernant tous les supports contrôlés physiquement peuvent être justifiées.

OP1.3.3	Les rapports d'audit et de surveillance sont systématiquement examinés afin de relever les anomalies et de mener des actions correctives le cas échéant.

Sécurité des technologies de l'information (OP2)	
Gestion des systèmes et des réseaux (OP2.1)	
OP2.1.1	Il existe un ou plusieurs plans de sécurité établis par écrit pour protéger les systèmes et les réseaux.
OP2.1.2	Le ou les plan(s) de sécurité sont régulièrement revus, testés et mis à jour.
OP2.1.3	Les informations sensibles sont protégées grâce à des stockages sécurisés, tels que
	– des chaînes de conservation bien définies
	– des sauvegardes stockées hors site
	– des moyens de stockage amovibles,
	– des procédures pour la mise au rebut des informations sensibles ou de leur support de stockage
OP2.1.4	L'intégrité des logiciels installés est vérifiée régulièrement.
OP2.1.5	Tous les systèmes sont à jour eu égard aux révisions, correctifs et recommandations relatives aux avis de sécurité.
OP2.1.6	Il existe un plan de sauvegarde des données établi par écrit qui
	– est systématiquement mis à jour
	– est testé régulièrement
	– implique des sauvegardes régulièrement programmées des logiciels et des données
	– exige des essais périodiques et la vérification de la capacité de restauration à partir des sauvegardes
OP2.1.7	Tout le personnel comprend ses responsabilité et est en mesure de les assumer dans le cadre des plans de sauvegarde.
OP2.1.8	Les modifications du matériel et des logiciels informatiques sont planifiées, contrôlées et établies par écrit.
OP2.1.9	Les membres du personnel des TI suivent les procédures lors de la création, la modification et la suppression des mots de passe, comptes et privilèges utilisateurs.
	– Une identification unique par utilisateur est nécessaire pour tous les utilisateurs des systèmes d'information, y compris les utilisateurs tiers
	– Les comptes par défaut et les mots de passe par défaut ont été supprimés des systèmes.
OP2.1.10	Seuls les services nécessaires sont exploités sur les systèmes – tous les services superflus ont été supprimés.
Outils d'administration des systèmes (OP2.2)	
OP2.2.1	Les nouveaux outils, procédures et mécanismes de sécurité sont systématiquement revus quant à leur applicabilité pour respecter la stratégie de sécurité de l'organisation.
OP2.2.2	Des outils et mécanismes sont utilisés pour l'administration sécurisée des systèmes et des réseaux et sont systématiquement revus et mis à jour ou remplacés. Par exemple,
	– les contrôles d'intégrité des données
	– les outils cryptographiques,
	– les scanners de vulnérabilité
	– les outils de vérification de la qualité des mots de passe
	– les programmes de détection de virus

	– les outils de gestion de processus
	– les systèmes de détection d'intrusion
	– les administrations sécurisées à distance
	– les outils de service réseau
	– les analyseurs de trafic
	– les outils de réponse en cas d'incident
	– les outils d'analyse judiciaire des données
Surveillance et audit de la sécurité des TI (OP2.3)	
OP2.3.1	Des outils de surveillance et d'audit des systèmes et des réseaux sont systématiquement utilisés par l'organisation.
	· L'activité est contrôlée par le personnel des TI
	· L'activité des systèmes et des réseaux est établie par écrit/ enregistrée
	· Les journaux sont révisés de façon régulière
	· Les activités inhabituelles sont traitées conformément aux règles ou procédures appropriées.
	· Les outils sont révisés et mis à jour régulièrement.
OP2.3.2	Les pare-feu et autres composantes de sécurité sont régulièrement audités afin de vérifier qu'ils respectent la politique.
Authentification et autorisation (OP2.4)	
OP2.4.1	Des contrôles d'accès et une authentification utilisateur appropriés (par exemple, permissions fichier, configuration réseau) conformes à la politique sont appliqués pour limiter l'accès des utilisateurs à
	· l'information,
	· aux utilitaires,
	· au code source des programmes,
	· aux systèmes sensibles,
	· aux applications et services spécifiques,
	· aux connexions réseau au sein de l'organisation,
	· aux connexions réseau extérieures à l'organisation
OP2.4.2	Il existe des politiques et des procédures établies par écrit sur l'utilisation des informations pour l'accès individuel et groupé afin de
	· définir les règles d'octroi du niveau d'accès approprié,
	· définir un droit d'accès initial,
	· modifier le droit d'accès,
	· résilier le droit d'accès
	· revoir et vérifier périodiquement les droits d'accès
OP2.4.3	Les méthodes/mécanismes de contrôle d'accès limitent l'accès aux ressources conformément aux droits d'accès définis par les politiques et procédures.
OP2.4.4	Les méthodes/mécanismes de contrôle d'accès sont régulièrement revues et vérifiées.
OP2.4.5	Des méthodes ou mécanismes sont prévus pour garantir que les informations sensibles n'ont pas été consultées, modifiées ou détruites de façon non autorisée.
OP2.4.6	Des mécanismes d'authentification sont utilisés pour protéger la disponibilité, l'intégrité et la confidentialité des informations sensibles. Par exemple avec

	· des signatures numériques
	· la biométrie
Gestion des éléments vulnérables (OP2.5)	
OP2.5.1	Il existe un recueil établi par écrit de procédures visant à gérer les éléments vulnérables, y compris
	· en sélectionnant des outils d'évaluation des éléments vulnérables, des listes de contrôle et des scénarios,
	· en les actualisant par rapport aux types d'éléments vulnérables et aux méthodes d'attaque connus,
	· en examinant les sources d'information sur les annonces de vulnérabilité, les alertes de sécurité et les notifications,
	· en identifiant les composantes de l'infrastructure à évaluer,
	· en programmant des évaluations des éléments vulnérables,
	· en interprétant les résultats et en y répondant,
	· en assurant le stockage et la suppression sécurisés des données sur les éléments vulnérables
OP2.5.2	Les procédures de gestion des éléments vulnérables sont suivies et régulièrement revues et mises à jour.
OP2.5.3	Des évaluations des éléments vulnérables de la technologie sont menées de façon périodique et les éléments vulnérables sont traités dès qu'ils sont identifiés.
Cryptage (OP2.6)	
OP2.6.1	Des contrôles de sécurité appropriés sont effectués pour protéger les informations sensibles pendant le stockage et au cours de la transmission, y compris
	· le cryptage des données pendant la transmission
	· le cryptage des données lors de l'écriture sur le disque
	· l'utilisation d'une infrastructure à clé publique
	· la technologie relative au réseau privé virtuel
	· le cryptage de toutes les transmissions basées sur l'internet
OP2.6.2	Des protocoles cryptés sont utilisés lors de la gestion à distance des systèmes, routeurs et pare-feu.
OP2.6.3	Les contrôles et protocoles de cryptage sont systématiquement revus, vérifiés et révisés.
Architecture et conception de la sécurité (OP2.7)	
OP2.7.1	L'architecture et la conception des systèmes pour les systèmes nouveaux et révisés intègrent des considérations concernant
	· les stratégies, politiques et procédures de sécurité
	· l'historique des compromissions de sécurité
	· les résultats des évaluations des risques en matière de compromission de la sécurité
OP2.7.2	L'organisation dispose de diagrammes actualisés qui présentent l'architecture de sécurité de toute l'entreprise et la topologie du réseau.

Sécurité du personnel (OP3)	
Gestion des incidents (OP3.1)	
OP3.1.1	Il existe des procédures établies par écrit pour l'identification, l'établissement de rapports et les réactions en cas d'incidents et de violations suspectés de la sécurité, y compris
	· des incidents basés sur les réseaux
	· des incidents liés à l'accès physique
	· des incidents liés à l'ingénierie sociale

OP3.1.2	Les procédures de gestion des incidents sont régulièrement testées, vérifiées et mises à jour.
OP3.1.3	Il existe des politiques et des procédures établies par écrit pour travailler avec les services répressifs.
Pratiques générales du personnel (OP3.2)	
OP3.2.1	Les membres du personnel adoptent de bonnes pratiques en matière de sécurité, notamment
	· la sécurisation de l'information dont ils sont responsables,
	· pas de divulgation des informations sensibles à autrui (résistance face à l'ingénierie sociale),
	· les compétences nécessaires pour utiliser les matériels et logiciels des technologies de l'information
	· l'application de bonnes pratiques concernant les mots de passe,
	· la compréhension et l'application des politiques et règles de sécurité,
	· l'identification des incidents et l'établissement de rapports
OP3.2.2	Tout le personnel à tous les niveaux de responsabilité met en œuvre les rôles et responsabilités qui lui ont été attribués en matière de sécurité de l'information.
OP3.2.3	Il existe des procédures établies par écrit pour l'autorisation et la surveillance du personnel travaillant avec des informations sensibles ou sur des sites où ces informations sont stockées. Il s'agit
	· des salariés
	· des contractants, partenaires, collaborateurs et personnel des organisations tierces,
	· du personnel de maintenance des systèmes
	· du personnel de maintenance des installations

Annexe E. Conseils simples[4]

CONSEILS IMPORTANTS DE SECURITE POUR LES PETITES ET MOYENNES ENTREPRISES

Voici les aspects essentiels des moyens de défense de votre entreprise

- ☐ Effectuer de vérifications de base lors de la sélection de l'ensemble de vos salariés et contractants (par exemple, à partir des références ou des recommandations)
- ☐ Connaître et consigner les actifs de valeur de votre organisation
- ☐ Disposer de politiques et procédures de sécurité concises, efficaces et clairement établies par écrit
- ☐ Dispenser des séances de formation de sensibilisation de base à la sécurité de vos salariés
- ☐ Installer les correctifs traitant les éléments logiciels vulnérables de façon automatique ou dès que possible, après avoir vérifié leur fonctionnalité
- ☐ Savoir qui accède à vos systèmes et pourquoi
- ☐ Utiliser des mots de passe forts et les changer régulièrement
- ☐ S'assurer que les fonctions anti-virus sont installées sur tous vos ordinateurs et postes mobiles et que votre système anti-virus est mis à jour automatiquement
- ☐ Utiliser des produits anti-virus différents pour votre serveur et vos ordinateurs clients
- ☐ Utiliser un système de filtrage de contenu pour vous protéger des spams, de l'hammeçonnage, des contenus malveillants et interdits
- ☐ Utiliser un pare-feu, surtout si vous disposez d'un accès internet à large bande
- ☐ Utiliser un système de défense réseau «tout en un» pour les petits réseaux

Mots de passe

Ce sont les clés permettant d'accéder à vos informations électroniques. Les informations qui ne sont pas protégées par un mot de passe peuvent être lues par tout le monde. Si vous choisissez des mots de passe «faibles», il est possible que quelqu'un les devine ou les décrypte. Voici quelques conseils pour choisir des mots de passe forts.

- Ouvrez le dictionnaire à une page choisie au hasard et choisissez un mot long (disons de quatre syllabes). Utilisez ce mot mais insérez le numéro de la page au milieu. Par exemple, si <multiplicité> figure à la page 345 de votre dictionnaire, votre mot de passe est <multi345plicité>. (Si vous oubliez votre mot de passe, vous pouvez vous souvenir de la page que vous avez sélectionnée.)
- Choisissez «une phrase de passe» qui a une signification pour vous. Par exemple, «mon zèbre s'appelle Spot et a 9 ans». Elle peut être

[4] L'objectif des informations fournies dans la présente annexe est de donner des conseils simples aux utilisateurs sur les questions de sécurité de base. Ces informations ont été compilées à partir des références [1], [6] et [10] de la bibliographie.

transformée en mot de passe <mzsaS&a9a>. Ce mot de passe est très fort parce qu'il contient des lettres, des chiffres et des caractères spéciaux. Il est extrêmement difficile à deviner.

Pour créer un mot de passe, il faut:

- utiliser au moins 8 caractères,
- veiller à changer de mot de passe régulièrement, par exemple, tous les mois,
- si un salarié quitte l'entreprise, son ancien mot de passe doit immédiatement être modifié,
- utiliser un mot de passe par application – ne jamais utiliser le même mot de passe pour tout.

D'autre part, différentes pratiques sont à proscrire avec les mots de passe.
Il est recommandé de:

- ne jamais noter un mot de passe!
- ne jamais utiliser votre nom, le nom de votre conjoint, les noms des enfants, votre plaque d'immatriculation, les dates d'anniversaires ou toute autre information sur vous ou votre famille qui soit publique ou qui puisse facilement être retrouvée avec un peu d'«ingénierie sociale»,
- ne jamais utiliser des codes spéciaux qui vous concernent, par exemple, votre numéro de téléphone, votre numéro de carte d'identité, le numéro de licence du logiciel, qui pourraient tous être retrouvés,
- ne jamais utiliser une série de chiffres ou de lettres identiques, par exemple <11111111>, dans un mot de passe et ne jamais utiliser le mot de passe <motdepasse> car c'est le premier qu'un pirate informatique essaiera,
- ne jamais divulguer votre mot de passe à quiconque,
- ne jamais utiliser un mot de passe par défaut fourni dans un logiciel – modifiez-le,
- ne jamais utiliser les fonctions «se souvenir du mot de passe» sur un ordinateur car les mots de passe enregistrés ainsi sont faciles à récupérer même pour des non initiés.

En résumé, les mots de passe doivent faire l'objet d'une grande attention. Choisissez un mot de passe fort, changez-en régulièrement et prenez-en soin.

Virus, ver et cheval de Troie

Les puristes diront qu'il s'agit de problèmes distincts mais d'un point de vue organisationnel, vous pouvez les traiter ensemble. L'essentiel est que tous peuvent endommager et endommagent réellement vos ordinateurs et les informations qu'ils contiennent. Toutefois, il est assez simple de les éviter. Utilisez un programme anti-virus. Tous les programmes anti-virus conviennent car ils fonctionnent tous plus ou moins de la même manière et font le même type de tâches. Le plus important est simplement d'en utiliser un.

Ce que la plupart des gens ne savent pas c'est que les programmes anti-virus doivent être actualisés. Cela implique des mises à jour quotidiennes – oui, quotidiennes – car les personnes qui écrivent ces programmes sortent de nouvelles versions tous les jours.

Si vous n'installez pas le logiciel anti-virus et ne le mettez pas à jour, vous êtes sûr à 100% d'être infecté par un virus tôt ou tard.

Quel que soit votre anti-virus, vous devez l'installer pour vérifier toutes les nouvelles données automatiquement. Ainsi, si vous récupérez des données sur une disquette, un CD ou sur l'internet, l'éventuelle présence de virus sera vérifiée avant qu'ils ne puissent causer des dommages.

La règle d'or est de détruire tous les fichiers ou données infectés par des virus. Certains programmes anti-virus prétendent désinfecter les fichiers mais cela n'est jamais garanti. Le plus sûr est de détruire le fichier vérolé. S'il s'agit d'un courrier électronique, détruisez-le systématiquement sans l'ouvrir!

Spam

Vous pouvez penser qu'il s'agit simplement d'une nuisance mais malheureusement les spams présentent également des dangers. Ils peuvent être:

- une porte d'entrée pour des fraudes
- des chaînes de courriers électroniques embêtants
- porteurs de codes cachés qui modifient les paramètres de votre ordinateur (par exemple, en vous dirigeant vers un site pornographique)
- porteurs de codes cachés qui transforment votre ordinateur en relais (c'est-à-dire que de nombreux spams sont envoyés à partir de votre ordinateur dans le monde entier) en envoyant ainsi des spams à toutes les adresses de vos clients dans le monde entier avec une nouvelle copie du spam/ver/ cheval de Troie joint à celui-ci!

En cas de code caché, il rentrera très probablement dans la catégorie «cheval de Troie» et pourra être intercepté par votre anti-virus. Toutefois, vous devez suivre certaines règles en matière de spams qui vous permettront de minimiser les risques.

- Si le courrier électronique ne présente de toute évidence aucune valeur et aucun intérêt pour vous ou votre organisation, qu'il est mal écrit, détruisez-le simplement sans l'ouvrir.
- Ne répondez jamais à un spam. Votre adresse de courrier électronique a été trouvée par un moyen quelconque et les spammers ne savent pas si vous existez réellement.
- Si vous répondez, vous confirmez votre existence et vous en recevrez beaucoup plus.
- Ne cliquez pas sur le lien «cliquez ici pour vous désinscrire de la liste de diffusion» dans le courrier électronique. Il s'agit habituellement d'un piège. Vous ne serez pas désinscrit, vous confirmerez simplement que vous existez.
- Ne communiquez votre adresse de courrier électronique qu'à des personnes de confiance.
- Cela est très difficile si vous gérez une entreprise car vous souhaitez que votre adresse soit largement diffusée. Prévoyez de disposer de deux adresses de courrier électronique; l'une publique et l'autre à usage personnel qui est minutieusement contrôlée.
- Si un site web vous demande votre adresse de courrier électronique, faites une rapide évaluation des risques. S'agit-il d'une organisation jouissant d'une renommée bien établie? Avez-vous déjà entendu parler de cette personne auparavant et une adresse postale est-elle indiquée sur le site

web? Sachez que les escrocs se font passer pour des entreprises tout à fait honnêtes.

- Les sites internet qui promettent de vous retirer des listes de diffusion de spam ne le font généralement pas. Ne vous en servez jamais

Une possibilité est de bloquer les spams. Des logiciels spécialisés de filtrage sont disponibles mais peuvent s'avérer trop onéreux pour les petites entreprises. Il vaut probablement mieux demander à votre fournisseur de service internet s'il peut – pour quelques euros de plus – assurer le filtrage des spams avec son propre dispositif. Toutefois, une petite mise en garde à ce propos: le filtrage des spams est autant un art qu'une science. Vous pouvez facilement bloquer des courriers tout à fait valides si les critères anti-spams sont trop stricts.

N.B. Si vous recevez un courrier électronique qui menace directement votre entreprise d'une façon ou d'une autre, par exemple menaces de chantage, contactez immédiatement la police la plus près de chez vous. Vous serez rapidement orienté vers une équipe formée pour traiter les menaces électroniques. Cela ne vous arrivera certainement pas, mais juste au cas où…

Logiciel espion (spyware)

Il s'agit de petits programmes qui sont insérés dans le système de l'ordinateur pour collecter secrètement des informations sur les utilisateurs/entreprises sans qu'ils en aient connaissance, et ce principalement à des fins publicitaires. Toutefois ce programme peut également récupérer des informations sur vos adresses de courrier électronique et même vos mots de passe et numéros de carte de crédit.

Il y a récemment eu des campagnes officielles de prévention sur les logiciels espions utilisés pour obtenir des informations sensibles sur le plan commercial, par exemple, des clauses de contrats.
Les logiciels espions sont à éviter et l'utilisateur averti tentera de les limiter ou de les supprimer entièrement. Deux applications disponibles sur l'internet vous permettront de supprimer les logiciels espions de votre ordinateur. Ils sont tous deux gratuits pour un usage personnel mais payants pour les entreprises. Il s'agit de:

- <Ad-aware> de Lavasoft
- Spybot

Il est recommandé de télécharger ces deux programmes et de les lancer au moins une fois par semaine. Vous serez surpris de ce qu'ils trouvent. (Et n'oubliez pas qu'ils doivent être également mis à jour!)

Pare-feu

Le terme «pare-feu» vient des barrières physiques érigées dans les bâtiments pour éviter la propagation des incendies. En informatique, un pare-feu est un élément qui agit comme une barrière pour empêcher tout accès non autorisé à un système informatique privé ou à partir de celui-ci. Imaginez une sorte de porte de sécurité et d'alarme antivol pour les ordinateurs. Il aide à limiter toutes les menaces intentionnelles présentées précédemment. Un pare-feu est aujourd'hui considéré comme un dispositif essentiel si vous disposez d'un ou de plusieurs ordinateurs connectés à l'internet.

Le pare-feu est soit un logiciel soit un matériel. Pour protéger les grands systèmes informatiques, il peut combiner logiciel et matériel.

Le principal élément est qu'un pare-feu vérifiera toutes les données entrant et même sortant de l'ordinateur pour s'assurer qu'elles sont légitimes. En résumé, un pare-feu est votre meilleur rempart contre les pirates informatiques. Pour prendre un exemple concret, un pare-feu pourrait empêcher que votre ordinateur soit pris d'assaut par un tiers et devienne un relais de spam. Il convient de rappeler que lorsque vous connectez votre ordinateur à l'internet, vous ouvrez 65 536 «portes» - ou pour utiliser le terme technique, «ports» - par lesquelles des données peuvent entrer dans votre ordinateur. Or vous souhaitez seulement disposer des ports nécessaires ouverts uniquement pour vous pour envoyer ou recevoir des données, puis qu'ils restent fermés le reste du temps.

Il s'agit d'un domaine informatique très complexe et il n'y a pas lieu de s'étendre ici sur ses principes et ses pratiques qui font l'objet de thèses de doctorat. Heureusement, les logiciels pare-feu sont à présent très abordables, conviviaux et facilement disponibles.
Si vous avez un seul ordinateur, achetez un pare-feu logiciel. Son installation est simple, il vous suffit d'accepter les paramètres par défaut. Si vous disposez de plusieurs ordinateurs connectés à l'internet, un pare-feu matériel pourrait être un meilleur investissement avec une installation entre tous vos ordinateurs et le câble qui sort vers l'internet. Les pare-feu matériels sont plus complexes et il est préférable qu'un expert se charge de son installation et de sa configuration. Un professionnel s'assurera que votre pare-feu ne vous empêche pas de vous connecter à l'internet.

(Les entreprises disposant d'un ou deux ordinateurs peuvent acheter des logiciels combinant pare-feu et anti-virus en un seul programme, qui présentent des avantages économiques et techniques pour les petites entreprises.)

Rustines logicielles

Peu connues, mais néanmoins très importantes, les rustines logicielles sont liées aux virus et au piratage informatique. Tous les logiciels ont leurs problèmes et leurs défauts. Dans la plupart des cas, les défauts sont si mineurs qu'ils peuvent être ignorés et n'auront probablement aucun impact sur l'entreprise. Certains défauts sont trop importants pour qu'ils soient ignorés.

Tous les producteurs de logiciels fournissent des rustines logicielles – à savoir des mises à jour du logiciel destinées à supprimer les problèmes de leur logiciel. Si vous disposez d'un seul ordinateur qui n'est connecté à rien (ni à un autre ordinateur, ni à l'internet ou autre), vous n'avez probablement pas à vous soucier des rustines logicielles tant que votre ordinateur fonctionne parfaitement.

Les problèmes ci-après concernent principalement le système d'exploitation de votre ordinateur. C'est le programme de base qui tourne au cœur de votre ordinateur. Vous utilisez certainement une version de Microsoft Windows, peut-être Apple OSX ou Unix/Linux. Tous ces systèmes d'exploitation doivent être réparés à l'aide de rustines logicielles de temps à autre. Mais beaucoup d'applications doivent aussi être réparés à l'aide de rustines logicielles de temps à autre. Les navigateurs internet et les programmes de messagerie doivent souvent être réparés à l'aide d'une rustine logicielle et il n'est pas rare que les progiciels de comptabilité habituels aient aussi besoin d'une rustine.

Si vous n'actualisez pas votre logiciel avec des rustines, vous risquez une panne du logiciel ou, s'agissant de votre navigateur ou logiciel de messagerie, de laisser des logiciels malveillants altérer votre ordinateur ou des utilisateurs malveillants prendre d'assaut votre ordinateur.

La plupart des fabricants de logiciels envoient une annonce par courrier électronique pour informer leurs clients des nouvelles rustines logicielles. Les annonces concernent des corrections qui peuvent être essentielles ou être appliquées à n'importe quel moment. Si vous recevez une alerte de rustine logicielle essentielle et qu'elle concerne un logiciel sur lequel votre entreprise compte, il vous est conseillé de l'installer dès que possible. La continuité de vos activités en dépend peut-être. Consultez également le site web du fabricant du logiciel pour vous informer sur les mises à jour.

De nos jours, la plupart des fabricants de logiciels fournissent des mises à jour automatiques via l'internet.

Sauvegardes

La sauvegarde est le processus consistant à faire une copie de données électroniques, comme une copie des fichiers de comptabilité. Pourquoi s'en inquiéter? Parce que les données électroniques sont très faciles à perdre, égarer ou détruire. Si vous perdez la seule copie de votre comptabilité électronique, comment ferez-vous marcher votre entreprise demain?

Un système formel et efficace de sauvegarde vous permettra d'éviter bon nombre des menaces naturelles ou involontaires citées précédemment. Vous pouvez copier vos données essentielles sur:

- des bandes (méthode ancienne mais toujours intéressante à envisager car vous pouvez continuer à les réutiliser)
- un autre disque dur (de préférence amovible)
- un CD (environ 700 Mo) ou un DVD (environ 4,3 Go)

Vous devriez envisager plusieurs sauvegardes des données critiques en utilisant trois générations de supports. Par exemple, en sauvegardant les données «fin de semaine» des trois dernières semaines en alternance de sorte que vous disposiez toujours de trois semaines (ou générations) de sauvegardes simplement au cas où vous deviez recréer le système. Un bon système de sauvegarde pour une entreprise (même composée d'une seule personne) serait:

- à la fin de chaque jour – sauvegarde de tous les fichiers qui ont été modifiés au cours de la journée
- à la fin de chaque semaine – sauvegarde de toutes les applications (comptabilité, correspondance, etc.)
- à la fin de chaque mois – sauvegarde du système d'exploitation également.

Si vous devez restaurer votre ordinateur après une panne catastrophique, vous utiliserez la dernière sauvegarde «fin de mois» pour recréer le système d'exploitation, puis vous restaurerez la dernière sauvegarde d'application «fin de semaine».
Enfin, restaurez chacune des sauvegardes «fin de journée» effectuées après la dernière sauvegarde «fin de semaine». Ainsi, vous aurez restauré l'ensemble du système. Si l'une des sauvegardes ne peut être lue (ce qui se produit étonnamment assez souvent quel que soit le moyen de sauvegarde), vous pouvez revenir à la copie précédente des trois copies et commencer à partir de là. Si cela se produit, vous ne pourrez restaurer la toute dernière version de vos fichiers de données. Il manquera inévitablement quelque chose qui sera sur le support en panne. Cette éventualité est néanmoins préférable à la perte de l'intégralité de vos précieuses données.

Ce type de processus de sauvegarde a été utilisé depuis que les ordinateurs ont été inventés et s'est avéré fiable. Des systèmes plus compliqués de sauvegarde peuvent être utilisés lorsque les données changent souvent ou ont une très grande valeur. Soyez prêts à changer si les risques de votre entreprise changent.

Conservez vos sauvegardes en lieu sûr. Elles sont aussi précieuses que vos données originales et font également l'objet des mêmes principes d'archivage intelligent. Ne les laissez pas dans un endroit où elles pourraient être volées ou endommagées. Et ne les laissez pas sur votre ordinateur. S'il explose ou prend feu, qu'adviendra-t-il de vos sauvegardes de sécurité? L'idéal est de conserver les sauvegardes dans un bâtiment totalement différent de celui de l'ordinateur. Si votre bureau était détruit par le feu, vous ne voudriez pas que vos sauvegardes connaissent le même sort!

Le problème qui peut se poser avec les sauvegardes est qu'elles ne soient pas correctement étiquetées avec la date et leur objet. Si cette sauvegarde doit ensuite être retrouvée de toute urgence…

Si vous avez de nombreuses sauvegardes sur différents supports, une solution est d'acheter un coffre-fort résistant au feu. Ce coffre-fort peut alors rester sur place mais vous devez savoir qu'après un incendie très vif, deux à trois jours d'attente peuvent être nécessaires avant que le coffre-fort soit assez refroidi pour l'ouvrir.

Vol d'informations et usurpation d'identité

Il s'agit d'un des délits en plus forte augmentation au Royaume-Uni et dans d'autres pays développés. Il a fait l'objet de beaucoup de publicité mais un point important n'a pas été mentionné. Le vol d'informations et l'usurpation d'identité peuvent toucher aussi bien les entreprises que les individus.

Pour une entreprise, il est vital de se défaire des informations obsolètes en toute sécurité, aussi bien sur support papier qu'électronique. Il est déjà arrivé que de petites entreprises disposant de leur propre site internet voient leur site détourné par quelqu'un qui a volé d'anciennes lettres sur papier à en-tête et a trouvé la signature des dirigeants. Cette pratique permet de faire de fausses lettres aux agences chargées de l'enregistrement des noms de domaine sur l'internet afin que le site web soit réenregistré à une nouvelle adresse physique. Une fausse entreprise est alors créée et des crédits sont contractés.

Des particuliers peuvent aussi être victimes d'usurpation d'identité avec intention frauduleuse. Même si vous ne serez pas considéré comme responsable d'une fraude évidente perpétrée par d'autres, le problème en cas d'usurpation d'identité est de retrouver de la crédibilité auprès des banques et autres organisations financières et notamment les agences de renseignement commercial.
Ce qu'il ne faut pas faire:

- ne donnez jamais d'informations personnelles sur l'internet, par courrier électronique, par téléphone ou par lettre à quiconque à moins d'être sûr que vous pouvez leur accorder votre confiance;
- rappelez-vous que les banques ne demandent jamais à leurs clients de confirmer leur mot de passe ou code d'accès par courrier électronique; ne fournissez jamais ce type d'informations;
- ne jetez jamais de documents personnels ou professionnels confidentiels sans les avoir déchirés et utilisez si possible une déchiqueteuse à double coupe (horizontale et diagonale);

- les supports électroniques ou magnétiques qui ne sont plus nécessaires doivent être physiquement endommagés de sorte qu'ils ne puissent être réutilisés.
- Si vous disposez de comptes bancaires professionnels ou de crédits non utilisés auprès d'anciens fournisseurs, clôturez-les car ils pourraient être exploités à des fins frauduleuses.

Dans tous les cas, vous devez contrôler minutieusement vos relevés bancaires et autres documents financiers ligne par ligne dès que vous les recevez. Tout versement ou débit étrange doit immédiatement faire l'objet d'une enquête. Votre banque se fera un plaisir de répondre à vos questions. Ils tiennent autant que vous à limiter les fraudes. Vous devez également vérifier régulièrement vos dossiers de crédits personnels ou professionnels pour les cas suivants:

- demandes concernant votre solvabilité de la part d'entreprises avec lesquelles vous n'avez jamais traité,
- observations de nature à discréditer votre solvabilité,
- notifications d'un changement d'adresse ou
- références à des décisions judiciaires, etc.

Réseaux sans fil

Les réseaux sans fil (dits WiFi) sont très attrayants pour les petites entreprises. Ils sont peu coûteux à installer, faciles à configurer, assurent une grande flexibilité et évitent des problèmes de câblage difficile et onéreux. Malheureusement, il est aussi très simple de mettre en place un réseau WiFi permettant que tout le monde lise vos informations professionnelles confidentielles.

Le principal risque est que toute personne dans la zone sans fil puisse utiliser votre réseau WiFi. Elle pourrait ainsi utiliser gratuitement votre connexion internet, saisir vos transmissions de données, par exemple, courriers électroniques, mots de passe, accéder aux fichiers de données sur vos ordinateurs ou même capter vos coordonnées bancaires sur l'internet. Un réseau WiFi non sécurisé présente un risque important d'espionnage industriel.

La mise en place d'un réseau WiFi dans votre entreprise doit être minutieusement planifiée et nécessitera probablement l'aide d'experts. Les présentes recommandations ne constituent pas un guide exhaustif pour l'installation d'un réseau. L'important est ici qu'un réseau WiFi peut et doit être installé de façon sécurisée afin que seuls vous et votre personnel puissiez l'utiliser et accéder/ échanger des données. Voici quelques conseils essentiels.

Tout d'abord, voici malheureusement quelques informations techniques importantes. Tous les réseaux WiFi doivent respecter la norme IEEE 802.11. Cette norme comporte plusieurs révisions. Les plus importantes pour vous sont la 802.11 G et 802.11N. La version «G» est applicable dès à présent et la version «N» est un peu plus loin. En entreprise, optez dès à présent pour la version «G» bien que des versions «pré N» soient désormais en vente mais ils pourraient être légèrement différents de la version finale «N». La norme «N» propose des vitesses de transmission beaucoup plus rapides et en théorie, de meilleures conditions de sécurité. N'optez pas pour les variantes «A» et «B» qui sont désormais obsolètes car elles sont plus lentes et moins sécurisées.

Ne vous fiez pas aux déclarations des fabricants en matière de performances. Vous bénéficierez au final généralement de la moitié de la vitesse de transmission sur la moitié de la distance à moins d'être dans des conditions de laboratoire. La construction du bâtiment peut avoir un impact sur les performances WiFi sachant que les bâtiments en pierre sont ceux qui rencontrent le plus de problèmes.

Ce dont vous aurez besoin:

- un routeur sans fil qui transmettra et recevra les signaux de données dans tout le bureau. Les plus sophistiqués peuvent être réglés de façon à ce que le signal soit limité pour couvrir uniquement vos locaux;
- une connexion à large bande, si vous n'en avez pas déjà une;
- un adaptateur sans fil pour chaque ordinateur. La plupart des ordinateurs portables modernes en ont un intégré mais les ordinateurs de bureau auront besoin d'un adaptateur externe. Il est recommandé que l'adaptateur sans fil puisse se raccorder directement à un port USB.

Lorsque l'entreprise dispose d'un serveur central de fichiers déjà installé avec une connexion internet, le routeur sera directement relié au serveur de fichier. Les petites entreprises peuvent acheter le routeur avec un modem à large bande intégré. On peut aussi acheter des «boîtes noires» plus sophistiquées combinant routeur et pare-feu pour une meilleure protection. Il est préférable d'acheter tout votre kit WiFi chez le même producteur. N'essayez pas d'agencer plusieurs matériels car si cela ne fonctionne pas, tous les fournisseurs se renverront les torts. Et évidemment, n'achetez pas une marque inconnue.

Ces notes techniques sont essentielles pour la sécurité:

- toutes les transmissions de données doivent être cryptées. N'utilisez pas le cryptage WEP mais privilégiez plutôt le WPA ou WPA2;
- utilisez une clé PSK pour instaurer une sorte de mot de passe entre vos ordinateurs et le routeur. Il est recommandé d'en utiliser une longue;
- créez un nom unique pour votre réseau WiFi dans tout le service;
- définissez des identifiants (SSID); créez vous-même un nom sécurisé de SSID;
- configurez votre routeur WiFi afin que votre SSID ne soit pas diffusé;
- n'utilisez jamais le nom SSID par défaut du fabricant;
- enregistrez les adresses MAC de vos ordinateurs auprès du routeur et créez une règle afin que seules les adresses MAC enregistrées puissent communiquer avec lui;
- assurez-vous que les systèmes d'exploitation de votre serveur et de vos autres ordinateurs supportent le système WiFi avant d'acheter le kit!

Si tout cela vous semble un peu compliqué, n'essayez pas d'installer votre réseau WiFi seul et faites appel à un expert. N'oubliez pas que vos données sont probablement votre principal atout et qu'il faut les protéger avec un réseau WiFi dûment sécurisé. Après tout, vous ne voulez certainement pas que votre réseau devienne un point d'accès public.

Tiers

Les PME font assez souvent appel à des tiers pour bon nombre d'activités. Généralement, il s'agit de conseils en gestion d'entreprise et marketing ainsi que de services de support informatique pour les systèmes critiques. Ces tiers ont la plupart du temps accès aux

informations confidentielles de l'entreprise ou à l'infrastructure systèmes et réseaux à des fins de maintenance. Il est essentiel que les entreprises garantissent la confidentialité de ces informations sur le plan contractuel mais également dans le cadre d'un processus officiel de gestion du contrôle d'accès. Au minimum, les PME doivent envisager les contrôles suivants lorsqu'elles ont recours à des tiers:

- signer un accord de confidentialité;
- fournir un accès sélectif aux informations sur la base du besoin de savoir, ce qui signifie que les tiers ne doivent avoir accès qu'aux informations qui sont absolument nécessaires pour leur travail;
- il NE faut PAS accorder d'accès permanent aux fournisseurs de support informatique à moins que cela ne soit explicitement exigé et nécessaire. L'accès doit être immédiatement supprimé à la fin des activités nécessaires. Les journaux d'audit doivent être imprimés et vérifiés afin de s'assurer que les activités qui ont été menées se sont limitées aux opérations de maintenance autorisées;
- demandez à votre fournisseur la possibilité d'examiner ses mesures de sécurité, notamment lorsque des informations internes et confidentielles sont traitées dans ses locaux.

Prestataires de services

Les prestataires de service sont généralement des fournisseurs de services internet, des fournisseurs de services applicatifs et des fournisseurs en télécommunications. Avant de choisir un prestataire de services, les personnes responsables devraient s'informer sur les réglementations établies par le fournisseur potentiel, par exemple quels sont les plafonds fixés pour la largeur de bande, si les courriers électroniques sont filtrés et le cas échéant, suivant quelles règles.

Les prestataires stockent généralement les données des utilisateurs pour leur facturation (nom, adresse, ID utilisateur, coordonnées bancaires) ainsi que les données de connexion et les contenus transmis (sur une période qui varie entre les prestataires).

Les utilisateurs devraient demander à leurs fournisseurs quelles données sont stockées et pendant combien de temps. Lors du choix d'un fournisseur, il faudrait tenir compte du fait que les fournisseurs européens doivent respecter les règlements en matière de confidentialité des données s'appliquant au traitement de ces informations.

Grâce à l'utilisation du cryptage, les utilisateurs peuvent empêcher les prestataires de pouvoir lire le contenu des données transférées.

Des contrôles supplémentaires peuvent être envisagés.

- En fonction de quels critères le prestataire a-t-il été choisi?
- Quelles mesures de sécurité le prestataire prend-il?
- Selon quels critères les courriers électroniques sont-ils filtrés par le fournisseur (fournisseurs de messagerie)? Du personnel est-il disponible 24 h/24 pour traiter les problèmes techniques et ce personnel est-il compétent?
- Le fournisseur est-il prêt à intervenir en cas de panne de l'un ou plusieurs de ses systèmes informatiques (plan d'urgence, concept de sauvegarde informatique)?
- Quel est le degré de disponibilité garanti par le prestataire (temps d'arrêt maximum)? Le prestataire vérifie-t-il régulièrement que les connexions avec les clients sont stables et si elles ne le sont pas, prend-il les mesures nécessaires?
- Que garantit le fournisseur en termes de sécurité de ses systèmes informatiques et ceux de ses clients?

Tout fournisseur devrait disposer systématiquement d'une politique de sécurité de l'information et de consignes de sécurité. Les utilisateurs externes devraient pouvoir consulter les consignes de sécurité. Le personnel du fournisseur devrait être informé des questions de sécurité informatique et avoir l'obligation de respecter les consignes de sécurité; il devrait également bénéficier d'une formation régulière (pas uniquement sur les questions de sécurité).

Protection des données et vie privée

Outre vos salariés, quel est selon vous le principal actif commercial de votre organisation qui n'est pas visible, très souvent sous-évalué, qui peut être utilisé à mauvais escient s'il se retrouve entre de mauvaises mains, et qui peut être perdu instantanément?

La réponse la plus probable est l'information. De bonnes pratiques en matière de sécurité de l'information permettent que les bonnes personnes voient et traitent les bonnes

informations professionnelles et au moment où elles en ont besoin. La législation exige désormais de veiller à sauvegarder correctement les informations détenues sur des personnes.

La loi de 1998 sur la protection des données est entrée en vigueur au Royaume-Uni le 1er mars 2000. Elle porte sur les données personnelles, à savoir, les informations sur des individus vivants identifiables ou des «personnes fichées».

Les principales exigences de cette loi sont résumées ci-dessous:

- évaluation du risque des informations de nature personnelle et sensible;
- identification des contrôles nécessaires pour la protection des données et de la vie privée;
- élaboration et mise en œuvre d'une politique de sécurité de l'information.

Références

1. *The fraud advisory Panel – Cyber crime what every SME should know about* [Groupe consultatif sur la fraude – ce que toutes les PME doivent savoir sur la cybercriminalité]
2. Jack A. Jones, CISSP, CISM, CIS - *An Introduction to Factor Analysis of Information Risk (FAIR) - A framework for understanding, analyzing, and measuring information risk* [Introduction à l'analyse factorielle des risques liés à l'information– Cadre pour comprendre, analyser et mesurer les risques liés à l'information]
3. ENISA - *Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises* (SMEs) [Méthodes d'évaluation et de gestion des risques: dossiers d'information pour les petites et moyennes entreprises (PME)]
4. ENISA - *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools* [Gestion des risques: principes de mise en œuvre et inventaire des méthodes et outils d'évaluation/gestion des risques]
5. ISO 27001
6. DTI – *Directors Guide for Information Security* [Guide à l'intention des dirigeants sur la sécurité de l'information]
7. Oxford Integrated Systems - *Security in an Uncertain World SME's and a Level Playing Field* [La sécurité dans un monde incertain; PME et situation équitable
8. COMMISSION DES COMMUNAUTÉS EUROPÉENNES – DIRECTION GÉNÉRALE - B6: Sécurité des télécommunications et des systèmes d'information - Manuel d'évaluation de la sécurité des technologies de l'information (ITSEM) Version 1.0
9. UK Department of Trade and Industry, *Information Technology Security Evaluation Criteria* (ITSEC) [Ministère du commerce et de l'industrie du Royaume-Uni – Critères d'évaluation de la sécurité des technologies de l'information (ITSEC)]
10. Leeds Council - *Information Assurance Guide and Questionnaire for Small & Medium Sized Businesses (SMEs)* [Guide et questionnaire sur l'assurance de l'information pour les petites et moyennes entreprises]
11. Russell Morgan - *Information Security for Small Businesses [*La sécurité de l'information pour les petites entreprises*]*
12. *Network and Information Security Report* – ICTSB / NISSG [Rapport sur la sécurité des réseaux et des informations]
13. RECOMMANDATION DE LA COMMISSION du 3 avril 1996 concernant la définition des micro, petites et moyennes entreprises
14. *The OCTAVE (SM) Method Implementation Guide Version 2.*0 [Guide de mise en œuvre de la méthode OCTAVE]
15. Charles A. Shoniregun, *Impacts and Risk Assessment of Technology for Internet Security – Enabled Information Small-Medium Enterprises* [Impacts et évaluation des risques de la technologie pour la sécurité de l'internet – informations pour les petites et moyennes entreprises]
16. Journal officiel de l'Union européenne (20.5.2003)
17. *Risk Management among SMEs Executive report of discovery research* [La gestion des risques au sein des PME – Rapport de synthèse des recherches] par Alpa A. Virdi (Novembre 2005) Institute of Chartered Accountants in England and Wales
18. Reputation: Risk of risks [La réputation: le risque des risques] (livre blanc de l'*Economist Intelligence Unit*) Décembre 2005
19. *Risk management service for SMEs* [Service de gestion des risques pour les PME] (lettre d'information) International Accounting Bulletin: 3, 24 mai 2006. ISSN: 0265-0223, Lafferty Publications Ltd
20. *Information Security Guide for Small businesses* [Guide sur la sécurité de l'information pour les petites entreprises] (Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), INFOSEC de l'office of Government Chief Information Officer (OGCIO) et le Technology Crime Division HK Police force of the HKSAR Government.)
21. http://sme.cordis.lu/home/index.cfm (SME TechWeb)
22. http://europa.eu.int/information_society/policy/ecomm/info_centre/documentation/legislation/index_en.htm#top (La société de l'information en Europe – portail thématique)