Small Business Standards

GUIDE DE MISE EN ŒUVRE

DE LA NORME DE GESTION DE LA SÉCURITÉ DES INFORMATIONS ISO/CEI 27001

À L'INTENTION DES PME

European DIGITAL SME Alliance

Président:
Fabio Guasconi

Coordinateur:
Guido Sabatini

Experts:

Georgia Papadopoulou

George I. Sharkov

David Bulavrishvili

Sergio Oteiza

Holger Berens

Ermal Çifligu

Sebastiano Toffaletti

Nanuli Chkhaidze

Yuri V. Metchev

Thorsten Dombach

Alexander Häußler

AVANT-PROPOS

L'Alliance européenne des PME numériques (European DIGITAL SME Alliance ou DIGITAL SME) est le plus important réseau européen de petites et moyennes entreprises du secteur des TIC : il représente environ 20 000 PME numériques. C'est une initiative conjointe de 28 associations nationales et régionales des PME numériques des États membres de l'UE et des pays voisins visant à inscrire les PME numériques au cœur de l'agenda de l'UE.

DIGITAL SME est membre de Small Business Standards (SBS), l'association européenne des parties prenantes concernées, qui représente les PME dans le domaine de la normalisation, conformément à l'Annexe III du Règlement 1025/2012 de l'UE. Pour progresser dans la mise en œuvre du Programme de travail 2017 de SBS, DIGITAL SME a élaboré, à l'intention des PME, ce Guide de mise en œuvre de la norme ISO/CEI 27001 relative au management de la sécurité de l'information.

Ce Guide a été élaboré par le Groupe de travail « WG27K » de DIGITAL SME, composé d'experts au fait des questions relatives à la normalisation du système de management de la sécurité de l'information qui comprennent bien les besoins des PME dans ce domaine. Ces experts ont été recommandés par les associations de PME de différents pays européens et ont été sélectionnés sur la base de leurs compétences afin de veiller à la diversité de la composition du groupe.

SBS et DIGITAL SME sont les uniques propriétaires de ce Guide gratuit et accessible au public. La diffusion en France est assurée par Digital SME France (contact@france.digitalsme.eu), représentant français de European Digital Alliance, association ouverte aux entreprises, syndicats et associations de TPE/PME ainsi qu'aux organismes de promotion dans le domaine du numérique.

TABLE OF CONTENTS

1. Introduction à la cybersécurité

Aujourd'hui, l'information est un produit de base pour la plupart des entreprises – et pour beaucoup le seul produit, tandis que d'autres sont très dépendantes du traitement de l'information pour les besoins de leurs activités.

Malheureusement, certaines personnes malveillantes tentent d'utiliser le besoin d'information à leur profit et récemment, de nombreux exemples de comportement illégal (attaques virales assorties de rançons (WannaCry, Petya), fuites de données personnelles de grandes entreprises (Equifax ou autres) et fuites d'outils d'espionnage d'organismes de renseignement ont été constatées.

Plus les menaces augmentent, plus les entreprises doivent se concentrer sur les moyens de protéger les informations qu'elles traitent, par exemple en adoptant ces mesures simples de protection:

- La mise en œuvre d'un mot de passe pour accéder aux ordinateurs et aux systèmes,
- L'installation d'un antivirus sur les postes de travail des utilisateurs finaux et les environnements serveur,
- La désactivation des clés USB au sein de l'entreprise ou,
- L'acquisition de solutions mieux adaptées et plus onéreuses.

Nombre de mesures sont efficaces pour protéger les systèmes, tandis que d'autres sont un pur gaspillage de ressources financières et humaines. Cela ne tient nullement au fait que les outils cités plus haut sont mauvais ou inefficaces. La difficulté majeure consiste à décider quels outils sélectionner, et à déterminer leur coût et la manière de les mettre en œuvre efficacement dans le cadre des activités de l'entreprise.

En raison de la complexité de l'environnement de l'information et des subtilités des flux d'information, de nombreuses entreprises comprennent désormais la nécessité d'avoir un personnel dédié, notamment les responsables de la sécurité de l'information, les professionnels de la cybersécurité, et les comités de sécurité de l'information. Certaines créent aussi des services/équipes spécifiques chargés de la sécurité de l'information et de la réponse aux incidents liés à la cybersécurité. Pourtant, de nombreuses entreprises ne sont pas convaincues de l'utilité de leurs investissements dans des mesures de protection.

Les carences en matière de cybersécurité peuvent causer de graves problèmes, qui se divisent principalement en trois grandes catégories :

La perte de disponibilité, nuisant aux activités de l'entreprise ;

- La perte de disponibilité, nuisant aux activités de l'entreprise ;
- La perte de confidentialité, pouvant nuire à la réputation de l'entreprise, voire entraîner une action en justice ;
- La perte d'intégrité, menant à l'utilisation de données incorrectes, voire falsifiées.

La cybersécurité est essentielle pour protéger les actifs des entreprises de tout type et de toute taille. Mais qu'entend-on exactement par cybersécurité ?

1.1 Définition de la cybersécurité

Il n'existe pas de définition officielle de cybersécurité, mais son sens se rapproche de celui de **sécurité de l'information**. On considère souvent que la cybersécurité englobe les aspects les plus techniques de la sécurité de l'information – visant elle-même à protéger les informations qui peuvent être stockées sur papier, sur ordinateur, et même celles conservées par les personnes elles-mêmes. La cybersécurité concerne d'abord la protection des informations stockées et leur traitement. Elle se définit comme une solution dans laquelle les risques associés à l'utilisation des technologies de l'information, intégrant l'ensemble des risques et des vulnérabilités, sont réduits à un niveau acceptable au moyen de mesures appropriées. Le facteur humain, y compris les intérêts nationaux, y joue également un rôle de plus en plus important. La cybersécurité implique donc l'emploi de mesures appropriées en vue de protéger la confidentialité, l'intégrité et la disponibilité de l'information et des technologies de l'information.

1.2 Termes et définitions

Pour une meilleure compréhension de ce Guide, les termes courants et spécifiques qui y sont employés peuvent être définis comme suit:

Actif
Tout ce qui appartient à l'entreprise et qui a de la valeur. Il existe de nombreux types d'actifs, par exemple : données, matériels informatiques, logiciels, fournisseurs de services, personnel et emplacements physiques.

Attaque
Forme délibérée de mise en danger. Par exemple : acte indésirable ou injustifié dans le but de tirer profit d'un tiers ou de lui nuire par une action sur un ensemble d'actifs.

Disponibilité
Propriété pour une information ou un traitement d'être accessible et utilisable à la demande par une entité autorisée.

Confidentialité
Caractéristique d'une information qui ne doit être accessible qu'à ceux dont l'accès est autorisé.

Contrôle
Mesure visant à modifier le risque. Les contrôles comprennent les processus, les politiques, les appareils, les pratiques, ou les autres actions qui peuvent modifier efficacement le risque.

Intégrité
Propriété pour une information d'être non altérée.

Sécurité de l'information
Ensemble de mesures permettant de protéger la confidentialité, l'intégrité et la disponibilité de l'information.

Risque (sécurité de l'information)
Risque qui a le potentiel d'exposer un actif opérationnel à des menaces susceptibles d'exploiter ses vulnérabilités, et donc de causer des dommages à l'entreprise.

Évaluation du risque (sécurité de l'information)
Processus général d'identification du risque, d'analyse du risque et d'évaluation du risque.

Traitement du risque (sécurité de l'information)
Processus consistant à modifier le risque – impliquant habituellement l'évitement du risque, le partage du risque, l'atténuation du risque ou l'acceptation du risque.

Menace
Cause potentielle d'incidents indésirables, susceptibles de causer des dommages.

Vulnérabilité
Faiblesse d'un actif ou d'un contrôle pouvant être exploité par une ou plusieurs menaces.

2. Champ d'application

Ce Guide a été rédigé pour les PME qui dépendent énormément des actifs technologiques et leur est applicable. Ses lignes directrices peuvent être facilement mises en œuvre par d'autres organisations, quelles que soient leur taille ou leur complexité.

Fondé sur le contenu de la norme ISO/CEI 27001, ce Guide décrit un ensemble d'activités pratiques qui peuvent contribuer de manière significative à établir ou à accroître les niveaux de sécurité de l'information au sein d'une PME. Ces mesures renforceront leur position sur le marché et faciliteront les possibilités de partenariats au sein des marchés locaux et de l'UE.

Toutes les activités énumérées garantissent le cycle de vie de la sécurité de l'information au sein de l'entreprise. Elles comprennent l'établissement, la planification, la mise en œuvre, la réalisation et l'amélioration de tous les processus connexes, fondés sur la culture du risque et de l'amélioration continue.

3. Management de la sécurité de l'information dans une PME

3.1 Étape 1: Établir les bases de la sécurité de l'information

Le management de la sécurité de l'information ressemble beaucoup à d'autres projets majeurs que les entreprises peuvent entreprendre. Avant de débuter toute activité, il est préférable de décider quelle forme elle doit prendre, son calendrier et la

participation du personnel. Un spécialiste de ce domaine et la direction doivent être les tout premiers instigateurs : ils doivent mettre en place les bases de toutes les autres activités.

La mise en œuvre des premières étapes nécessite d'impliquer la direction, qui doit être chargée d'établir les fondements de la sécurité de l'information. Cette tâche incombe au responsable de la gestion de l'information. Les propriétaires des systèmes et les propriétaires des informations doivent également être tenus informés des progrès de la réalisation de cette tâche. Vous trouverez ci-dessous la description détaillée du personnel auquel on peut attribuer un rôle dans la gestion sécurisée de l'information.

3.1.1 Étape 1.1 Attribuer les rôles et les responsabilités

Dans chaque entreprise et pour chaque activité, l'existence de rôles et de responsabilités clairement attribués est essentielle. Les start-ups ou les petites entreprises considèrent souvent que la sécurité de l'information est un processus autonome, et un processus qui ne dépend pas de leur participation. Certains ont tendance à l'ignorer complètement.

Lorsqu'on décide de prendre des mesures pour définir ou réviser le management de la sécurité de l'information au sein d'une entreprise, il est important de définir et d'officialiser les rôles et les responsabilités avant de pouvoir aller plus loin. Toutes les étapes ultérieures comportent des « rôles généralement impliqués », et leurs responsabilités RACI (Responsible, Accountable, Consulted, Informed ou Responsable d'Exécution, Responsable de validation, Consulté, Informé) sont suggérées entre parenthèses.

Cette étape décrit dans leurs grandes lignes les principaux rôles du management de la sécurité de l'information et les responsabilités associées. Il est à noter que les entreprises les plus petites peuvent confier plusieurs rôles à la même personne ou les externaliser (à la seule exception de la direction). Préalablement à l'application de ce Guide, toutes les entreprises doivent attribuer spécifiquement et officiellement les rôles et les responsabilités de la sécurité de l'information en fonction de leur structure et de leur culture.

La direction

En dernier ressort, la responsabilité de la gouvernance de la sécurité de l'information incombe à la direction, qui fait partie de la gouvernance générale. La direction a pour tâche principale de veiller à ce que la sécurité de l'information appuie la réalisation des objectifs de l'entreprise en démontrant son alignement avec la création de valeur de l'entreprise, la gestion adéquate de ses ressources et les mesures correspondantes de ses performances. Il n'est pas nécessaire que la direction connaisse chaque actif de l'entreprise, mais elle doit avoir une connaissance générale des actifs critiques et de leur valeur pour les activités de l'entreprise.

La direction comprend traditionnellement le président directeur général (PDG), le directeur d'exploitation (DE) ou le conseil d'administration, selon la structure de l'entreprise. Aux fins du présent Guide, il convient de décider qui doit remplir ces rôles.

LES PERSONNELS CHARGÉS DES DIFFÉRENTS RÔLES DE LA SÉCURITÉ DE L'INFORMATION PERTINENTS POUR L'ENTREPRISE DOIVENT CONSIGNER PAR ÉCRIT ET RECONNAÎTRE LEURS RESPONSABILITÉS ET LEURS TÂCHES.

Une matrice RACI peut aider à préciser l'attribution des responsabilités et peut inclure:

- La détermination des besoins en matière de sécurité de l'information et leur classification
- La performance de l'évaluation des risques
- La définition, la mise en œuvre et la maintenance des mesures de sécurité
- L'acceptation du risque résiduel
- La documentation du système de sécurité (normes, procédures, etc.)
- La rédaction de la politique de sécurité et sa mise à jour
- La surveillance du système de sécurité
- Les plans d'amélioration de la sécurité
- Les plans de sensibilisation et de formation
- Les plans de continuation d'activité

Pour chacune de ces tâches, les responsabilités suivantes doivent être attribuées aux rôles identifiés:

- Responsible (referred to as 'R') to carry out the task. There should be at least one person responsible for each task (who might delegate it for assistance);
- Responsable de validation (appelé 'A'): celui qui approuve l'achèvement complet de la tâche
- Consulté (appelé 'C'): son opinion peut être nécessaire pour réaliser la tâche, dans le cadre d'une communication bilatérale. On le considère généralement comme un expert
- Informé (appelé 'I'): il est informé des progrès de la réalisation de la tâche dans le cadre d'une communication unilatérale

Le comité directeur de la sécurité de l'information

Dans certains cas, les PME peuvent mettre en place un comité directeur de la sécurité de l'information composé de parties prenantes de l'ensemble des principaux services de l'entreprise. Il est conseillé de doter le comité d'une charte, qui est principalement

un outil permettant aux décideurs-clés de parvenir à un consensus. Le comité directeur de la sécurité de l'information peut travailler de concert avec la direction et sera responsable des activités d'audit et de surveillance.

Au stade de la mise en place d'un comité directeur de la sécurité de l'information, il est souhaitable d'impliquer les responsables qui rendent compte à la direction et de programmer des réunions trimestrielles. Le comité doit se réunir pour traiter plusieurs questions relatives à la sécurité de l'information, comme:

- Les normes de sécurité et l'approbation des procédures ;
- La revue de l'analyse des risques et le plan de traitement des risques;
- Les résultats d'audit et les mesures associées;
- La surveillance du plan de sécurité de l'information;
- L'objectif de sécurité de l'information et les indicateurs de performance;
- La planification de séances de sensibilisation et de formation;
- Les interventions d'urgence.

Directeur/responsable de la sécurité de l'information

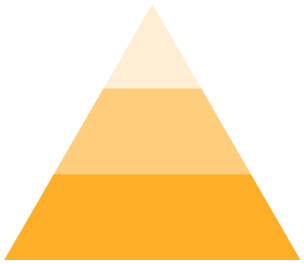
Bien que la sécurité de l'information concerne chaque service de l'entreprise, il est de plus en plus courant d'avoir un directeur de la sécurité de l'information qui coordonne les actions appropriées. Ce rôle peut être tenu par n'importe quel cadre supérieur (par exemple : directeur informatique ou directeur de la technologie) ayant une solide connaissance des flux d'information.

La sécurité de l'information étant rarement une discipline générale du management, le directeur de la sécurité de l'information explique à la direction les principaux aspects qui y sont liés, avant l'acceptation de la stratégie de sécurité de l'information. Obtenir l'engagement de la direction est un élément indispensable de la sécurité de l'information. L'une des activités essentielles est d'aligner les objectifs de l'entreprise et ceux de la sécurité de l'information. Citons, parmi les autres responsabilités : identifier les budgets, utiliser les modèles risques/avantages pour l'évaluation et le traitement des risques, rédiger les politiques et les procédures de sécurité de l'information et examiner les résultats des activités de surveillance.

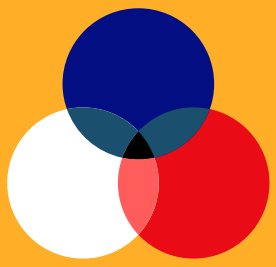
Le directeur de la sécurité de l'information est également chargé de promouvoir la sensibilisation à la sécurité de l'information, et peut aussi devoir assumer d'autres responsabilités, notamment la mise en place des canaux de communication et de comptes rendus. Le succès de la sécurité de l'information dépend beaucoup de la communication, à la fois interne et externe.

Les directeurs/responsables de la sécurité de l'information jouent un rôle de tout premier plan lors de l'application de ce Guide : ils doivent être sélectionnés pour leurs compétences et leur expérience dans ce domaine. Leur profil, s'il est dédié à ce rôle, peut aller de directeur de la sécurité à directeur de la sécurité de l'information. Pour tous renseignements complémentaires sur leurs profils professionnels et les compétences, se référer au document «CWA 16458 Profils informatiques professionnels européens».

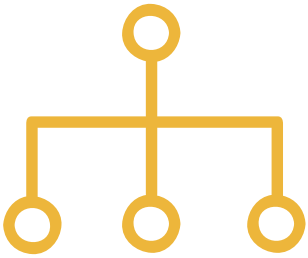
UN COMITÉ DIRECTEUR DE LA SÉCURITÉ DE L'INFORMATION PEUT OFFRIR LES AVANTAGES SUIVANTS :



Une coordination plus forte entre différents départements de l'entreprise



Une diffusion plus efficace de la culture de sécurité de l'information, puisqu'il y a davantage de services directement impliqués



Une vue plus globale lors de la prise de décision, car tous les domaines dépendent du comité

L'établissement d'une routine d'examen et de vérification de l'état de la sécurité de l'information et de son développement

AU STADE DE LA MISE EN PLACE D'UN COMITÉ DIRECTEUR DE LA SÉCURITÉ DE L'INFORMATION, IL CONVIENT DE PRENDRE EN COMPTE CE QUI SUIT :

- Chaque service doit être représenté par l'autorité décisionnaire appropriée, afin d'éviter les déséquilibres entre les différents services si certains domaines ne sont pas représentés par leurs responsables
- L'ordre du jour de la réunion doit être planifié et distribué à l'avance
- Les réunions doivent se tenir périodiquement (tous les trois mois) et de manière systématique
- Les règles de la réunion doivent être établies, notamment toutes les décisions relatives à la personne qui doit la présider et les modes de règlement des conflits potentiels
- Les décisions pertinentes sur la sécurité de l'information doivent être prises par ce comité
- Les calendriers doivent être respectés

Propriétaires des systèmes et des informations
Les entreprises plus structurées peuvent avoir besoin d'identifier plusieurs personnes chargées de réaliser au quotidien certaines tâches pour protéger les systèmes d'information qu'elles contrôlent : ce sont les «propriétaires des systèmes». Néanmoins, les propriétaires de l'entreprise en charge des processus et des données doivent participer à la définition de leurs besoins de protection, quels que soient les systèmes d'information : ce sont les « propriétaires des informations ». Ces deux catégories doivent aider l'entreprise en veillant à ce que les contrôles de sécurité de l'information soient en place et fonctionnent de manière adéquate.

Habituellement, les propriétaires sont en droit d'apporter des changements à tout ce qu'ils possèdent : améliorations du système, création de raccourcis, etc. Toutefois, ces décisions doivent toujours tenir compte des impacts sur la sécurité de l'information. Pour que ce modèle fonctionne, il convient d'indiquer clairement qui sont les propriétaires des systèmes et les propriétaires des informations au sein de l'entreprise. Cela commence par une approche a minima du directeur informatique et du directeur d'exploitation, qui sont tous deux impliqués. De plus, l'entreprise peut souvent avoir des difficultés à trouver des propriétaires des systèmes et des informations aux niveaux inférieurs de la hiérarchie – personnes qui décident de l'amélioration d'un actif ou de raccourcis. Il lui faut alors déléguer les pratiques décisionnelles et avoir une culture cohérente.

Personnel
La réussite de la sécurité de l'information repose sur la formation adéquate du personnel. Les employés et les entrepreneurs doivent avoir une parfaite connaissance des raisons justifiant l'environnement de contrôle qui les entoure, de façon à pouvoir maintenir la sécurité de l'information au bon niveau et ne pas la compromettre.

Les employés et les fournisseurs doivent être capables de reconnaître un comportement inhabituel et de signaler rapidement tout problème éventuel au directeur de la sécurité de l'information afin de réduire au minimum le préjudice que pourrait subir l'entreprise. Très souvent, les employés et les fournisseurs sont les cibles d'attaques. Par conséquent, avoir un personnel formé améliore considérablement l'environnement général de la sécurité de l'information. Ce personnel peut aussi être capable de transformer ces connaissances et cette expertise en culture organisationnelle.

3.2 Étape 2: Comprendre ce qui doit être protégé

À partir de cette étape, le Guide complétera la description de chacune des tâches suggérées pour la gestion sécurisée de l'information au sein d'une entreprise en donnant des exemples (figures, tableaux, etc.). Ces exemples aideront le lecteur à comprendre le Guide.

Avant d'appliquer toute mesure de sécurité de l'information, l'entreprise doit avoir une idée de départ précise des objets qui ont réellement de la valeur pour elle. Ces objets, définis généralement comme des **actifs**, peuvent globalement se diviser entre informations (voir *Étape 2.1*), actifs immatériels et autres actifs (voir *Étape 2.2*), matériels.

Le principal objectif de cette action est de décrire les principaux actifs qui sont gérés par l'entreprise et qui nécessitent une protection. C'est particulièrement important lors de l'identification des relations entre les actifs et de la définition des responsabilités.

Rôles généralement impliqués: direction (A), propriétaires des informations (C), propriétaires des systèmes (C), directeur/responsable de la sécurité de l'information (R).

3.2.1 Étape 2.1 Identifier les informations utilisées

Il est utile d'établir une **carte des actifs**, en commençant par les actifs immatériels : les informations de l'entreprise.

Approche descendante

L'entreprise peut choisir l'approche « descendante», dans laquelle les informations (encadrés blancs ci-dessous) sont identifiées alors qu'elles circulent dans les processus (encadrés de couleur ci-dessous).

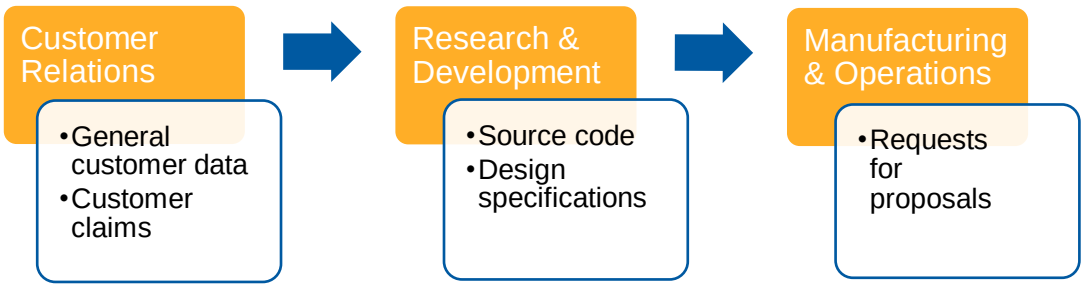
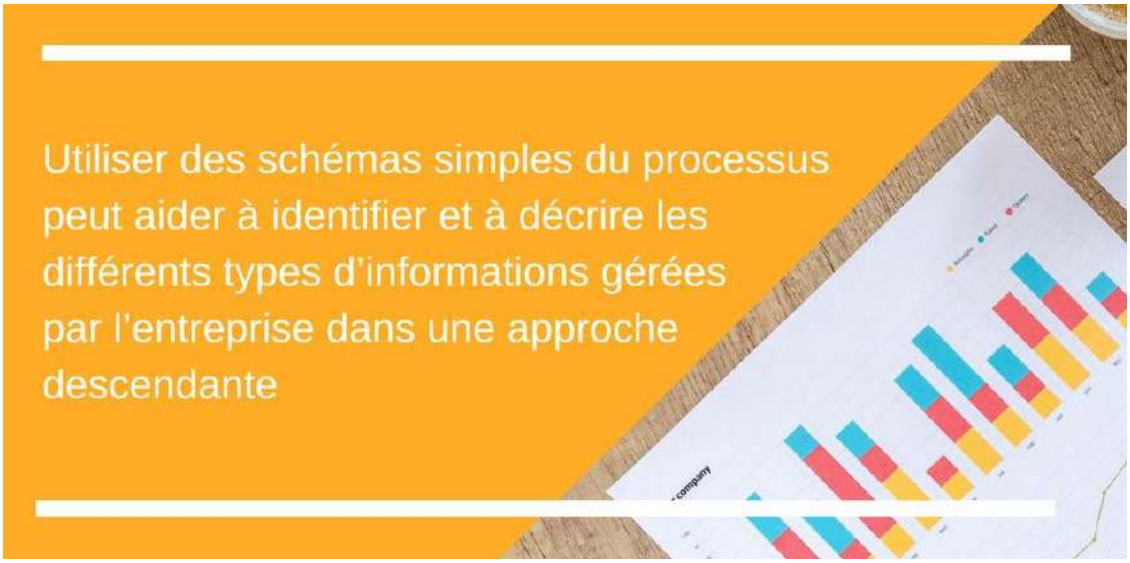


Figure 1: Exemple de carte d'actifs faisant référence à des informations hypothétiques au sein d'une entreprise donnée

Pour une utilisation optimale de l'approche descendante, l'entreprise doit bien comprendre ces processus, c'est-à-dire connaître leur nature, savoir qui est responsable de chaque processus, etc.

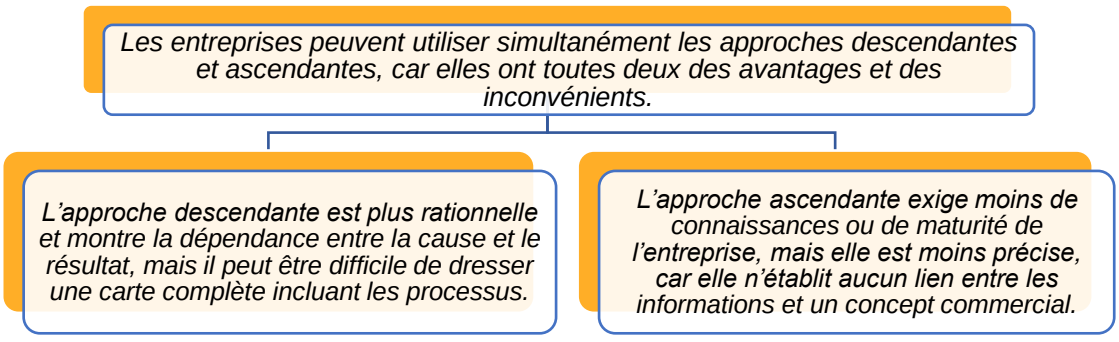


Le lien entre les activités de l'entreprise et les informations peut être précisé clairement, en commençant par une vue d'ensemble des processus et en descendant jusqu'aux actifs informationnels. Les propriétaires des informations (habituellement les directeurs commerciaux ou de services) sont les personnes les mieux placées pour répertorier et évaluer la pertinence de ces informations au sein de l'entreprise. Il est judicieux d'avoir un court entretien avec chaque propriétaire d'informations pour avoir une vue complète des informations gérées par l'entreprise.

Approche ascendante

L'approche descendante exige une bonne compréhension des processus organisationnels, qui n'est pas nécessaire pour l'approche « ascendante », qui peut être utilisée par n'importe quelle entreprise, quel que soit son niveau de maturité. Lors de la mise en œuvre une approche ascendante, le point de départ idéal est la réponse à la question: « Quelle sorte d'information l'entreprise gère-t-elle en général ?». Cette question peut être posée à toute personne qui a une vue d'ensemble de l'entreprise. La liste ci-dessous devrait permettre de s'assurer que tout ce qui est important est bien pris en compte:

a) Données personnelles (nom, adresses, numéro de sécurité sociale, effectifs salariés, etc.);
b) Données personnelles sensibles (diagnostics de santé, opinions politiques, données des cartes de paiement, ou autres);
c) Données stratégiques de l'entreprise (plans d'activités, prévisions, état budgétaire avant publication officielle, etc.);
d) Données du projet/conception (conception du produit, code source propriétaire, etc.);
e) Autres données de l'entreprise (données de surveillance, statistiques de production, renseignements fiscaux ou autres)



Après avoir établi la carte des actifs, l'entreprise doit bien connaître ses actifs informationnels au niveau conceptuel, quel que soit le matériel informatique (stockage ou traitement) utilisé.

3.2.2 Étape 2.2 Identifier les autres actifs utilisés

Les informations utilisées peuvent être stockées, traitées, ou transmises à l'aide de plusieurs autres actifs, principalement (mais pas exclusivement) technologiques. Ces

actifs sont généralement les couches logicielles qui tournent sur les systèmes d'information, mais il peut aussi s'agir de dossiers papier, de disques ou de services assurés par les fournisseurs de services externes. L'approche ascendante est habituellement nécessaire pour les identifier correctement, à savoir impliquer le personnel informatique et les administrateurs d'application (qu'ils soient, ou non, officiellement désignés comme propriétaires des systèmes). Il est vivement conseillé de ne pas négliger les actifs clés, qui appartiennent au moins aux catégories suivantes d'actifs:

1) Terminaux (ordinateurs portables, ordinateurs de bureau, tablettes, smartphones), serveurs et appareils ;
2) Logiciels destinés à l'utilisateur final (à l'exception des suites bureautiques ou des systèmes d'exploitation) ;
3) Fournisseurs de services (y compris le personnel, les fournisseurs d'hébergement/d'accès et de services Cloud) ;
4) Personnel (employés directs et de la sous-traitance) ;
5) Emplacements physiques (bureaux et salles d'ordinateurs). Those elements can also be investigated initially during a top-down interaction with information owners as described in the previous step, just after defining information related to processes and then refined with the system owners.

Ces éléments peuvent également être examinés pendant l'interaction descendante avec les propriétaires des informations, décrite dans l'étape précédente, juste après avoir défini les informations liées aux processus, puis affinées avec les propriétaires des systèmes.

L'exemple ci-dessus pourrait donner la liste structurée suivante:

SOFTWARE	HARDWARE	PERSONNEL	PROVIDERS	LOCATIONS
CRM application	Production servers	Internal staff	Cloud provider	Main offices
ERP application	Testing servers		TLC provider	
Shared folders	Staff PCs			
	Staff smartphones			

Figure 2: Exemple de carte d'actifs identifiant les actifs clés autres que les informations au sein d'une entreprise donnée

3.2.3 Étape 2.3 Comprendre les liens entre les informations et les autres actifs

Une fois tous les actifs clés identifiés, déterminer ceux qui sont utilisés pour certaines informations constitue un moyen simple mais efficace pour comprendre ce qui nécessite une protection et plus tard, le niveau de protection nécessaire.

Pour cela, on peut créer une matrice simple, comme celle ci-après : les cellules remplies indiquent un lien entre les actifs et les informations. Les cellules vides indiquent l'absence de lien.

	Données générales clients	Réclamations clients	Code source	Spécifications de conception	Demandes de proposition
Application CRM					
Serveurs de production					
Serveurs de test					
Ordinateurs du personnel					
Smartphones du personnel					
Dossiers partagés					
Application ERP					
Personnel interne					
Fournisseur de services Cloud					
Fournisseur TLC					
Bureaux principaux					

Tableau 1 : Exemple de matrice pour identifier les liens entre l'information et les autres actifs

Ces relations étant clairement établies, la carte des actifs est achevée. Elle sera très utile pour les étapes suivantes. Bien sûr, il est possible de recueillir davantage d'informations pour chaque actif, jusqu'à dresser un inventaire complet des actifs pouvant être utilisés afin d'améliorer leur gestion. Souvenez-vous que la carte des actifs doit être constamment actualisée, sinon elle perdra rapidement de son utilité.

3.3 Étape 3: Évaluer les risques liés à la sécurité de l'information

L'évaluation des risques liés à la sécurité de l'information a pour principal objectif de détecter à l'avance ce qui pourrait causer des problèmes au niveau des actifs et avoir un impact négatif sur la trésorerie, les obligations légales ou la réputation d'une entreprise. Cette étape est cruciale pour comprendre les menaces auxquelles l'entreprise est confrontée, car elle lui permettra de mettre en œuvre des contrôles visant à éviter et à contenir les menaces ou à résoudre le problème si elles se matérialisaient. En hiérarchisant les risques, chaque entreprise peut concentrer des ressources défensives là où elle risque de subir les pertes les plus importantes, optimisant ainsi l'efficacité de ces ressources.

Rôles généralement impliqués: direction/comité directeur de la sécurité de l'information (A), propriétaires des informations (C), propriétaires du système (C), directeur/responsable de la sécurité de l'information.

3.3.1 Étape 3.1 Comprendre la valeur des actifs

Pour que la carte des actifs (voir *Étape 2.3*) soit parfaitement adaptée au processus d'évaluation des risques, il convient d'ajouter un élément clé : l'évaluation de l'importance de chaque actif au sein de l'entreprise.

Pour évaluer les actifs, il est possible d'utiliser différentes échelles (par exemple : effectuer une évaluation faible/moyenne/élevée). Pour affiner cette analyse, on peut évaluer l'impact en intégrant des critères supplémentaires, comme:

- Les exigences juridiques
- Les intérêts économiques ou commerciaux
- La réputation (image publique)
- La sécurité

La manière la plus simple de réaliser cette évaluation est de commencer par les informations qui ont été définies et d'examiner au moins deux des propriétés principales liées à la sécurité de l'information : la **disponibilité et la confidentialité.** On peut ajouter l'intégrité, mais dans les contextes les plus simples, on peut considérer qu'elle est étroitement liée à la disponibilité. Il convient de procéder à l'évaluation de base des informations définies à l'*Étape 2.1 (*chaque propriétaire d'informations utilisant le tableau ci-après comme référence) en attribuant une valeur à la disponibilité et à la confidentialité de chaque poste d'information identifié.

	Valeur faible	**High Valu**
Disponibilité (D)	L'indisponibilité de cette information pourrait-elle avoir un impact grave sur les activités de l'entreprise ou sa réputation ?	
	Non	**Oui**
Confidentialité (C)	La diffusion non autorisée de cette information pourrait-elle causer des dommages concurrentiels à l'entreprise ou enfreindre des lois ou des obligations contractuelles majeures ?	
	Non	**Oui**

Tableau 2 : Évaluation des actifs au regard leurs disponibilité et de leur confidentialité.

L'application du tableau ci-dessus à l'exemple pourrait donner les valeurs suivantes:

Données générales clients	Réclamations clients	Code source	Spécifications de conception	Demandes de proposition	Ordres d'achat
A: faible C: élevée	A: faible C: faible	A: faible C: élevée	A: faible C: élevée	A: élevée C: faible	A: faible C: élevée

Table 1: Example of evaluation of information for its availability and confidentiality

Dans la mesure où les valeurs principales de tous les autres actifs sont liées aux informations qu'ils stockent, traitent ou transmettent, cette première évaluation peut s'appliquer à tous les actifs rattachés aux informations évaluées dans la carte des actifs. Ceci suppose que leur relation avec les informations dont les valeurs sont les plus élevées indique leur valeur réelle pour l'entreprise, comme indiqué ci-dessous.

	Données générales clients	Réclamations clients	Code source	Spécifications de conception	Demandes de proposition	
	A: faible C: élevée	A: faible C: faible	A: faible C: élevée	A: faible C: élevée	A: élevée C: faible	
Application CRM						**A: faible, C: élevée**
Serveurs de production						**A: élevée, C: élevée**
Serveurs de test						**A: faible, C: élevée**
Ordinateurs du personnel						**A: élevée, C: élevée**
Smartphones du personnel						**A: faible, C: élevée**
Dossiers partagés						**A: faible, C: élevée**
Application ERP						**A: élevée, C: faible**
Personnel interne						**A: élevée, C: élevée**
Fournisseur Cloud						**A: élevée, C: élevée**
Fournisseur TLC						**A: élevée, C: élevée**
Principaux bureaux						**A: élevée, C: élevée**

Tableau 4 : Exemple de matrice pour l'identification complète de la relation entre les actifs et leur évaluation en matière de disponibilité et de confidentialité

Cette carte des actifs remplie et améliorée, quel que soit la façon dont elle est représentée, fournit une bonne réponse à la question de savoir ce que la sécurité de l'information doit protéger et à quel point, selon le rôle réel de l'actif.

3.3.2 Étape 3.2 Évaluer le type de contexte dans lequel l'entreprise évolue

La connaissance approfondie de l'environnement dans lequel l'entreprise évolue est d'une importance capitale au stade de la définition des exigences en matière de sécurité de l'information. L'ENISA, l'Agence européenne chargée de la sécurité des réseaux et de l'information, a élaboré un modèle de menaces cybernétiques, utile lors de l'évaluation de toutes les menaces auxquelles les entreprises risquent d'être confrontées. La typologie de l'ENISA comporte les catégories de menaces suivantes:

a) Catastrophe (par exemple séisme, inondation, incendie);
b) Catastrophe (par exemple séisme, inondation, incendie);
c) Attaque physique (par exemple vol, sabotage);
d) Juridique (par exemple violation de règlement, ordonnance de tribunal);
e) Dommage involontaire (par exemple fuite d'information, perte d'un appareil);
f) Pannes-dysfonctionnement (par exemple panne ou dysfonctionnement de matériel)?;
g) Pannes-dysfonctionnement (par exemple panne ou dysfonctionnement de matériel)?;
h) Écoute illicite-interception-détournement (par exemple espionnage,«homme au milieu»)

L'applicabilité de ces menaces doit être évaluée en tenant compte des données historiques des incidents (si elles sont disponibles) et de l'expérience du personnel. Une évaluation de ce type pourrait au moins établir, par exemple, comment les conditions suivantes s'appliquent à l'environnement de l'entreprise:

1) Dans quelle mesure les locaux de l'entreprise sont-ils exposés aux catastrophes naturelles ou aux incidents (inondations, incendies, séismes)?
2) Dans quelle mesure les locaux de l'entreprise sont-ils exposés aux interruptions de service (connexion Internet, coupure électrique, grèves)?

3) Dans quelle mesure le personnel est-il fiable (faible rotation, pas d'agitation, cohésion des équipes)?
4) Dans quelle mesure les règlements ou les exigences contractuelles impactent-ils l'entreprise?
5) Dans quelle mesure l'entreprise est-elle exposée aux erreurs humaines du personnel?
6) Dans quelle mesure l'entreprise est-elle dépendante des fournisseurs externes?
7) Dans quelle mesure les services TIC exposent-ils l'entreprise à l'Internet?
8) Dans quelle mesure la réputation de l'entreprise est-elle importante?

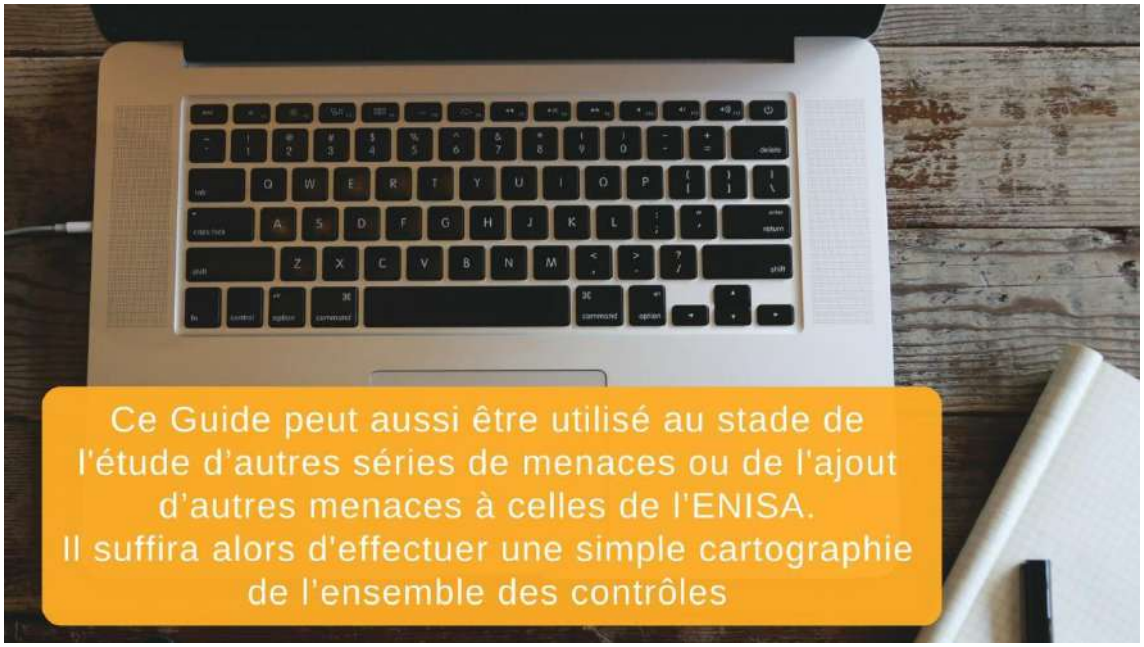
Les réponses à ces questions (qui peuvent donner des valeurs élevées/faibles/nulles), obtenues en consultant les informations pertinentes et les propriétaires des actifs, peuvent être vraiment utiles pour déterminer les menaces auxquelles l'entreprise risque de faire face, en reliant directement 1 à a, 2 à b, etc. à la typologie des menaces cybernétiques de l'ENISA. Ces considérations doivent être séparées des mesures en place dans l'entreprise.

Toutes les menaces dont les réponses aux questions correspondantes n'ont pas abouti à l'attribution de la valeur «Aucune» et qui sont applicables à l'un quelconque des actifs identifiés décrits dans le tableau ci-après, doivent être considérées comme des causes de risques potentiels pour l'entreprise.

	Disaster	Outages	Physical attack	Legal	Unintentional damage	Failures-malfunction	Nefarious-activity-abuse	Eavesdropping-interception-hijacking
Hardware	X		X		X	X	X	
Software				X	X	X	X	X
Service providers		X		X		X		X
Personnel	X	X		X			X	X
Physical locations	X		X					

Tableau 5 : Exemple de matrice à utiliser pour évaluer le type de contexte dans lequel l'entreprise évolue

Par exemple, si la réponse à la question 3) était « Faible », l'**attaque physique** c) associée à la menace correspondante s'appliquerait aux actifs de matériels informatiques et d'emplacements physiques. Dans la carte des actifs donnée en exemple (Figure 2), ce serait les serveurs de production, les serveurs de tests, les ordinateurs du personnel, les smartphones du personnel et les bureaux principaux.



3.3.3 Étape 3.3 Identifier les contrôles déjà en place

Les contrôles de sécurité de l'information sont des éléments fondamentaux de la diminution des risques : correctement mis en œuvre, ils peuvent être d'une très grande efficacité. Dans bien des cas, l'entreprise a déjà mis en place plusieurs contrôles, mais ils sont nombreux et ne doivent pas être pris en compte uniquement au niveau de l'entreprise, mais souvent également au niveau des actifs, afin d'identifier toute faille de protection.

L'Annexe A de la norme ISO CEI/27001 est une remarquable liste de contrôles, établie spécifiquement pour permettre à l'entreprise de vérifier « tous » les contrôles potentiellement applicables. A l'**Annexe A de ce Guide,** cette liste a été simplifiée pour s'appliquer aux PME, tout en gardant trace de la référence aux contrôles d'origine de la norme ISO CEI/27001. Il convient d'indiquer, pour chaque contrôle de cette liste, s'il est déjà complètement appliqué ou non (par précaution, une application partielle sera considérée comme une non-application) à chaque groupe d'actifs lié à un poste d'information.

3.4 Étape 4: Concevoir, appliquer et surveiller les contrôles de sécurité de l'information

Dès que l'entreprise sait exactement quels sont les actifs à protéger et comment ils sont déjà protégés, elle peut décider quels sont les nouveaux contrôles à mettre en œuvre ou les contrôles à améliorer. La direction/le comité directeur de la sécurité de

l'information doit évaluer les mesures qu'il est impératif de prendre pour chaque risque avec, pour chaque solution, un calendrier et un financement. La plupart des propositions émanent habituellement du directeur/responsable de la sécurité de l'information. Les mesures de protection retenues doivent être efficaces et d'un bon rapport coût-efficacité.

Rôles généralement impliqués: direction/comité directeur de la sécurité de l'information (A), propriétaires des informations (R), propriétaires des systèmes (R), personnel (R), directeur/responsable en sécurité de l'information (R).

3.4.1 Étape 4.1 Identifier les contrôles à mettre en œuvre et établir un plan de sécurité de l'information

Choisir les contrôles à mettre en œuvre dans un environnement spécifique est la décision la plus difficile à prendre en matière de sécurité de l'information. Quelque soit le contexte, aucune combinaison de contrôles n'est parfaite, parce qu'il est susceptible d'engendrer des coûts supérieurs à ce qui est nécessaire, de générer de nombreux contrôles, de donner naissance à des incidents difficiles à prévoir, etc.

Conformément aux étapes précédentes et selon les bonnes pratiques en la matière, ce Guide propose en Annexe A de classer les contrôles dans deux catégories principales :

1. **Les contrôles de base**, idéalement à mettre en œuvre dans chaque situation;
2. **Les contrôles discrétionnaires**, à mettre en œuvre pour protéger les actifs de grande valeur, éventuellement susceptibles de faire l'objet de menaces.

Les contrôles de base sont regroupés dans la première section de l'Annexe A (A.1) et, sauf cas particulier, doivent toujours être mis en œuvre. L'Annexe X de ce Guide propose un exemple idéal de contrôle de base : la **politique de sécurité de l'information**. Une fois rempli, ce document de politique doit être approuvé officiellement par la direction de l'entreprise afin d'identifier correctement la priorité et les ressources au sein de l'entreprise.

Les contrôles discrétionnaires sont regroupés dans la deuxième section de l'Annexe A (A.2). Chaque contrôle y est associé aux menaces qu'il atténue dans la troisième section de l'Annexe A (A.3). Si la cellule de menace correspondante de la section A.3 ne contient aucune valeur, le contrôle n'atténue pas la menace de manière significative. Si la cellule contient la valeur « Secondaire », il l'atténue raisonnablement. Enfin, si la cellule contient la valeur « Principale », le contrôle est plus efficace. Comme une valeur a été attribuée à chaque actif à l'*Étape 3.1* et qu'elle a été associée aux menaces applicables à l'*Étape 3.2*, ces éléments peuvent simplement aider les utilisateurs à décider d'appliquer ou non un contrôle. Si un actif a une valeur élevée de confidentialité ou de disponibilité OU s'il est exposé à une menace hautement probable, il convient de n'appliquer que les contrôles ayant la valeur « Principale » pour cette menace spécifique. Si un actif a à la fois une valeur élevée de confidentialité ou de disponibilité ET est exposé à une menace hautement probable, il peut être intéressant d'envisager d'appliquer aussi les contrôles ayant la valeur « Secondaire » pour cette menace spécifique.

Par exemple, les smartphones du personnel – dont la valeur dans le tableau 4 est D : Faible; C : Élevée – sont des matériels informatiques et sont exposés à une menace d'attaque physique « Faible ». Tous les contrôles qui ont une relation «Principale» avec la menace d'attaque physique devront s'appliquer aux smartphones du personnel ainsi qu'aux contrôles de base. Ceci implique:

- A2.06 La gestion des supports amovibles;
- A2.10 La sécurité physique ;
- A2.11 La protection contre les menaces de l'environnement?;
- A2.12 La maintenance des équipements?;
- A.2.16 Les sauvegardes

Les contrôles appliqués, détectés à l'étape précédente, et ceux qui résultent des trois catégories ci-dessus mentionnées, devront être vérifiés **au niveau de chaque actif.** Lorsqu'un contrôle semble moins efficace que ce qui est recommandé ou est absent, il convient de le noter et de procéder à une analyse approfondie. La liste de ces contrôles constitue la base de l'établissement du **Plan de sécurité de l'information**, qui permettra à l'entreprise d'améliorer de manière ciblée la protection de la sécurité de l'information. Ce plan de sécurité doit comporter davantage d'éléments qu'une simple liste de contrôles, et pourrait inclure par exemple un ensemble d'actions avec les propriétaires concernés, les périodes, les coûts, et d'autres informations. Il peut être aussi une simple feuille de calcul contenant les champs suivants :

Code	*Id*
Source	*Source activity*
Action description	*Descriptive text*
Owner	*Function or person*
Cause	*Activity motivation*
Priority	*Low*
Status	*Open/Closed*
% progress	*0%-100%*
Resource	*Costs, personnel*
Start date	*dd/mm/yy*
End date	*dd/mm/yy*
Notes	*Other annotations*

Tableau 6 : Modèle de suivi des actions à mettre en œuvre au titre du Plan de sécurité de l'information

3.4.2 Étape 4.2 Gérer le Plan de sécurité de l'information

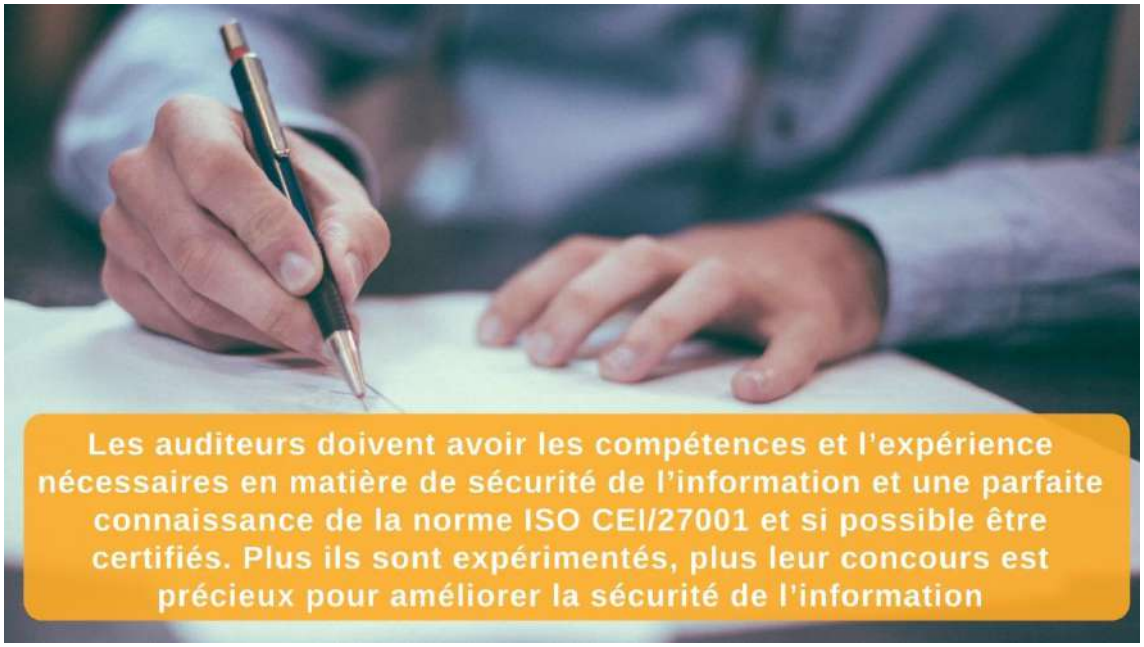
Une fois le Plan de sécurité de l'information approuvé, la responsabilité de sa surveillance périodique (par exemple mensuelle ou trimestrielle), afin d'évaluer s'il progresse bien et s'il inclut la participation la plus large possible d'autres parties intéressées, incombe au directeur/responsable informatique. Cette surveillance doit prendre la forme d'une réunion formelle d'un comité (comité directeur de la sécurité de l'information, par exemple) : tous les professionnels impliqués doivent rendre compte de leurs progrès, de leurs difficultés et des modifications à apporter au plan. Le plan doit être actualisé en conséquence et, si des modifications importantes exigeant de nouvelles ressources y sont apportées, soumis à nouveau à l'approbation de la direction. Même en l'absence de modifications importantes, le plan doit à nouveau être approuvé par la direction périodiquement (au moins une fois par an, si possible avant

la finalisation des budgets de l'année suivante afin de permettre une affectation correcte des ressources).

Le plan doit également inclure les résultats des nouvelles actions suggérées ou exigées par les activités réalisées à l'*Étape 4.3* ci-après.

3.4.3 Étape 4.3 Contrôler la sécurité de l'information

Effectuer, au moins une fois par an, des **audits de la sécurité de l'information** permet de s'assurer que la sécurité de l'information est satisfaisante. Les auditeurs devront être sélectionnés parmi un panel d'experts indépendants, qui seront chargés de vérifier la conformité des processus de la sécurité de l'information aux exigences internes et externes. Si l'audit est réalisé en interne, l'auditeur ne devra pas assumer de responsabilités opérationnelles en management de la sécurité de l'information, afin d'éviter tout conflit d'intérêts.



À l'issue de l'audit, la direction de l'entreprise doit recevoir un rapport contenant :

- Les non-conformités, c'est-à-dire, les points sur lesquels l'entreprise ne respecte pas la norme ;
- Les possibilités d'amélioration, c'est-à-dire les recommandations devant permettre à l'entreprise de travailler de manière encore plus sécurisée (même si elle respecte déjà la norme).

Les non-conformités et les actions déjà mises en œuvre doivent être soigneusement analysées, afin d'éviter qu'elles ne se reproduisent. Les actions déjà mises en œuvre doivent être consignées dans la version actualisée du Plan de sécurité de l'information parallèlement aux actions nécessaires pour corriger les non-conformités. Les possibilités d'améliorations doivent être évaluées et, le cas échéant, intégrées également dans le Plan de sécurité de l'information, si cela est jugé pertinent, généralement avec une priorité inférieure à celle des actions visant à corriger les non-conformités.

3.4.4 Étape 4.4 Surveiller la sécurité de l'information

Après avoir défini et conçu les protections de l'étape précédente, l'entreprise peut reprendre ses activités habituelles. Pour garantir l'efficacité du système, les activités de surveillance aideront à limiter les écarts par rapport au Plan de sécurité de l'information initial.

La méthode la plus pratique pour mener à bien les activités de surveillance consiste à établir des indicateurs d'objectif ou de performance simples mais efficaces, qui peuvent être régulièrement actualisés. Ces indicateurs peuvent être basés sur des objectifs ou des contrôles: ils sont essentiellement constitués de formules de calcul des seuils qui doivent déclencher une action quand ils sont dépassés ou atteints. Il est important d'attribuer la responsabilité d'appliquer régulièrement la formule aux indicateurs. La norme ISO/CEI 27004 peut être utile pour mener à bien cette tâche.

Les indicateurs d'objectif sont les indicateurs les plus simples à mettre en place. On peut les utiliser pour mesurer l'atteinte d'un objectif pertinent pour l'entreprise, comme obtenir la conformité aux présentes lignes directrices ou à la réglementation/norme pertinente, un niveau ou un état de service lié à la sécurité. Ils doivent être vérifiés à des intervalles de quelques mois.

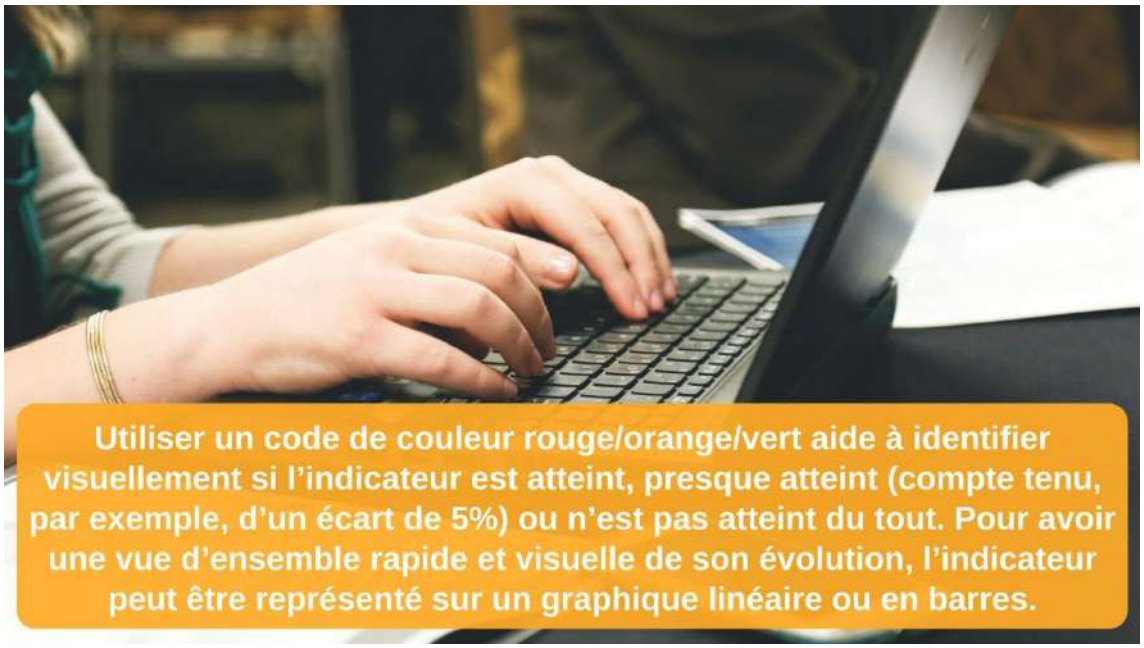
Les indicateurs de performance peuvent être liés à certaines valeurs de performance des processus de la sécurité de l'information (par exemple, évaluation des risques) ou à l'efficacité des contrôles. Dans ce dernier cas, les contrôles de base proposés à l'Étape 3.1 peuvent être associés à des indicateurs comme ces exemples:

Contrôle	Formule de l'indicateur	Cible	Périodicité
Politique de sécurité de l'information	% des employés qui ont eu communication de la politique	100 %	Annuelle
Organisation de la sécurité de l'information	Nombre de réunions du comité directeur de la sécurité de l'information	4	Annuelle
Sensibilisation à la sécurité de l'information, formation	% des employés qui ont reçu une formation,		
Nombre d'actions de sensibilisation à la sécurité	100 %	Annuelle	
Inventaire des actifs	% d'actifs inscrits à l'inventaire des actifs dans le mois suivant leur acquisition	100 %	Trimestrielle
Protection contre les logiciels malveillants	Nombre de postes de travail infectés/nettoyés	1	Mensuelle
Correction de la vulnérabilité des logiciels	Nombre de correctifs de sécurité critiques restant à appliquer	0	Mensuelle
Sécurité dans les contrats de fournisseurs	% de contrats comportant des clauses spécifiées liées à la sécurité de l'information	100 %	Trimestrielle

Tableau 7 : Suggestions de périodicité de surveillance des contrôles

Ce ne sont là que quelques exemples de base. Chaque entreprise doit déterminer systématiquement ses propres indicateurs.

Ces indicateurs, que l'on peut suivre sur une simple feuille de calcul, peuvent être régulièrement examinés par le directeur/responsable de la sécurité de l'information ou présentés au comité directeur de la sécurité de l'information.



À chaque cible doit correspondre un délai. D'autres seuils peuvent varier dans le temps et être fixés à une valeur inférieure à la cible initiale et augmenter avec la maturité du processus ou du contrôle concerné.

Le comité directeur de la sécurité de l'information peut contrôler périodiquement l'état et le développement du management de la sécurité de l'information.

4. Certification ISO/CEI 27001

L'approche proposée jusqu'à présent est étroitement liée aux exigences de la norme ISO/CEI 27001, comme le suggère le tableau de correspondances ci-après.

L'éventuelle absence de correspondance entre la norme internationale et ce Guide, est due à l'approche simplifiée adoptée par les auteurs du Guide, qui vise à supprimer les aspects les plus formels et les plus méthodologiques tout en se concentrant sur les aspects les plus pratiques.

Principaux chapitres de la norme ISO/CEI 27001 2013		Digital SME Guide steps
4.1	Compréhension de l'organisation et de son contexte	Step 3
4.2	Compréhension des besoins et des attentes des parties intéressées	Step 2
4.3	Détermination du domaine d'application du système de management de la sécurité de l'information	N/A
4.4	Système de management de la sécurité de	N/A

Principaux chapitres de la norme ISO/CEI 27001 2013		Digital SME Guide steps
	l'information	
5.1	Leadership et engagement	N/A
5.2	Politique	*Baseline control A1.01*
5.3	Rôles, responsabilités et autorités au sein de l'entreprise	Step 1
6.1	Actions liées aux risques et opportunités	Step 2 Step 3
6.2	Objectifs de sécurité de l'information et plans pour les atteindre	N/A
7.1	Ressources	N/A
7.2	Compétence	N/A
7.3	Sensibilisation	*Baseline control A1.03*
7.4	Communication	*Discretionary control A2.01*
7.5	Informations documentées	N/A
8.1	Planification et contrôles opérationnels	Step 4
8.2	Appréciation des risques de sécurité de l'information	Step 2 Step 3
8.3	Traitement des risques de sécurité de l'information	Step 4
9.1	Surveillance, mesures, analyse et évaluation	Step 4
9.2	Audit interne	Step 4
9.3	Revue de direction	
10.1	Non-conformité et actions correctives	Step 4
10.2	Amélioration continue	

Tableau 2: Contenu principal de la norme ISO CEI/27001 : 2013

Il conviendra toutefois de se pencher sur ce genre de problème (absence de correspondance) si l'obtention d'une certification officielle selon la norme ISO/CIE 27001 devient un objectif à poursuivre après avoir effectué le management de la sécurité de l'information pendant un certain temps en se basant sur ce Guide. Plus précisément, il conviendra de réaliser les activités supplémentaires décrites ci-dessous après l'Étape 1.1, présentées dans le chapitre 3.

4.1.1 Étape 1.2 : Établir un Système de management de la sécurité de l'information (SMSI)

Un système de management de la sécurité de l'information (SMSI) doit être considéré comme une approche plus formelle du management de la sécurité de l'information que celle décrite dans ce Guide. Un SMSI contiendra les politiques, procédures, principes directeurs et ressources et activités associées, collectivement gérés par une entreprise pour protéger ses informations. La direction doit être directement impliquée dans la planification d'un SMSI, qui introduit davantage de formalisme mais permet de progresser vers une certification internationalement reconnue pour une partie de l'entreprise. Il convient d'être vigilant lorsque l'on choisit cette partie, car son extension aura un impact direct sur les coûts de certification. Il est possible de choisir la totalité de l'entreprise, mais ce n'est pas le seul choix possible, puisque les services et les processus clés peuvent être considérés comme prioritaires en fonction des stratégies

commerciales de l'entreprise. Noter qu'il est également possible de ne certifier qu'une partie d'un SMSI plus large.

Il est indispensable d'impliquer dès que possible la direction dans la définition des grandes lignes de tout SMSI afin d'obtenir non seulement son accord mais aussi les ressources nécessaires. A cet égard, les différentes étapes de l'avancement de la mise en œuvre devront faire l'objet de rapports réguliers, tenant compte des délais fixés.

Au cours de cette phase, des objectifs mesurables et liés à l'entreprise doivent être proposés et sélectionnés. Ces objectifs, comme le reste du SMSI, doivent toujours viser l'amélioration continue, itération après itération.

4.1.2 Autres elements

L'approche de la gestion des documents à respecter dans le cadre d'un SMSI formel (et pour chaque système de management) exige également que chaque document produit:

- contienne des métadonnées complètes (au minimum, titre, date, auteur);
- repose sur des formats et des modèles établis?;
- soit sous le contrôle des changements/versions?;
- soit distribué au public visé.

Une déclaration d'applicabilité conforme aux exigences du point 6.1.3 d) de la norme ISO/CEI 27001 doit être produite et tenue à jour. Le modèle de sélection des contrôles proposé dans ce Guide représente un bon point de départ, mais doit comporter au minimum la justification de toute inclusion ou exclusion de chaque contrôle.

Une revue formelle de la direction, comprenant tous les éléments spécifiés au point 9.3 de la norme ISO/CEI 27001, doit aussi être périodiquement effectuée. Elle doit adopter la même approche que celle suggérée à l'*Étape 3.2*, mais doit aussi être explicitée.

Il est également possible d'ajouter une activité formelle de certification par une tierce partie. La marche à suivre peut être la même que pour un audit interne, tout en mettant à profit un point de vue compétent et externe sur le SMSI.

5. Références et ressources publiquement accessibles

Références

- ISO/IEC 27000 family – Information security management systems (Famille ISO/CEI 27000 – Systèmes de gestion de sécurité de l'information). Disponible en ligne en version anglaise sur: https://www.iso.org/isoiec-27001-information-security.html
- CEN CEN Workshop Agreement (CWA) 16458 on European ICT Professional Profiles (CWA Profils professionnels informatiques européens). Disponible en ligne en version anglaise sur: ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA%2016458.pdf. et en version française sur: http://www.ecompetences.eu/site/objects/download/6422_EUICTProfessionalProfilesCWAFR.pdf

Ressources librement accessibles

- BSI. ISO/IEC 27001 for small and medium-sized businesses (SMEs) (BSI. ISO/CEI 27001 pour les petites et moyennes entreprises (PME)). Disponible en ligne en version anglaise sur: https://www.bsigroup.com/en-GB/iso-27001-information-security/ISO-27001-for-SMEs/
- Centre for Cyber Security Belgium. Cyber Security Guide for SMEs (Le Centre pour la cybersécurité Belgique. Cybersécurité – Guide pour les PME). Disponible en ligne en version anglaise sur : https://ccb.belgium.be/en/document/guide-sme - et en version française sur : https://ccb.belgium.be/fr/document/guide-pour-les-pme
- European ENISA (European Union Agency for Network And Information Security) ou Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information. Information security and privacy standards for SMEs (Normes sur la sécurité de l'information et la vie privée pour les PME). Disponible en ligne en version anglaise sur : https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport
- *ENISA. Security guide and online tool for SMEs when going Cloud (Le guide de sécurité de l'ENISA et l'outil en ligne pour les PME passant au cloud). Disponible en ligne en version anglaise sur : https://www.enisa.europa.eu/news/enisa-news/enisa2019s-security-guide-and-online-tool-for-smes-when-going-cloud - et en version française sur https://www.enisa.europa.eu/news/enisa-news/prs-in-french/le-guide-de-securite-de-l'enisa-et-l'outil-en-ligne-pour-les-pme-passant-au-cloud*
- *ENISA. A simplified approach to Risk Management for SMEs (Approche simplifiée de la gestion des risques pour les PME). Disponible en ligne en version anglaise sur: https://www.enisa.europa.eu/publications/archive/RMForSMEs*
- *ETSI. NIS Directive Implementation – ETSI TR 103 456 – technical report released by ETSI's technical committee on Cybersecurity (TC CYBER) (ETSI. Mise en œuvre de la directive NIS – ETSI TR 103 456 – rapport technique publié par le comité technique sur la cybersécurité de l'ETSI (TC CYBER). Disponible en ligne en version anglaise sur :* http://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf
- ISO. Publicly available standards (including ISO/CEI 27000) (ISO. Normes disponibles publiquement, y compris ISO/CEI 27000). Disponible en ligne en version anglaise sur: http://standards.iso.org/ittf/PubliclyAvailableStandards/

ANNEX A

A.1 Baseline controls

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
01	**Information security policy**	5.1.1 5.1.2	An information security policy should be decided, agreed, published and communicated to all employees and to relevant third parties. The information security policy should be reviewed at a given frequency or in case significant changes occur to keep suitability, adequacy and effectiveness. *Suggested review frequency: annual*
02	**Information security organisation**	6.1.1 6.1.2	Roles and responsibilities of employees, contractors and any other party towards information security should be defined and documented while keeping duties and areas of responsibility segregated to limit damages arising from a single person's misbehaviour.
03	**Information security awareness, education and training**	7.2.2	All employees and relevant third parties should be periodically educated and made aware of information security threats. They should also be periodically trained according to the information security policy and procedures established by the organisation. *Suggested training frequency: yearly*
04	**Asset inventory**	8.1.1 8.1.2 8.1.3 8.1.4	A centralised asset inventory should be established, maintained and frequently reviewed. Ownership and responsibility for all assets should be identified, documented, accepted and implemented. A clear procedure for handling of all assets assigned to employees or a third party should be established and ensure traceability of those assets in all their lifecycle. *Suggested review frequency: monthly*
05	**Information classification, labelling and handling**	8.2.1 8.2.2 8.2.3	Information should be classified, labelled and handled according to its direct value for the organisation as well as to the current legislation. A procedure for information labelling and handling should be defined and applied by all information owners of the organisation. *Suggested classification levels: public, internal, confidential*
06	**User identification**	9.2.1 9.2.2	Information systems and services users should be uniquely identified through a formal registration and de-registration procedure for granting and revoking access.
07	**User authorisation**	9.2.3 9.2.5 9.2.6	The allocation and use of privileges to information systems and services users should be controlled and periodically reviewed. Users should only be provided with minimum rights needed to perform their duties. Any change of access privileges should be handled according to a strict procedure, subject to information owner's approval.
08	**User authentication**	9.2.4 9.3.1 9.4.1 9.4.2 9.4.3	Information systems and services users should be confidentially assigned credentials to authenticate themselves. Those credentials and the information systems verifying them should be robust enough to minimise the success of guessing attempts by unauthorised personnel. *Suggested credentials strength: 8 characters not from dictionary*

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
09	**Asset siting**	11.2.1 11.2.2 11.2.3 11.2.6	All assets carrying data or supporting information services should be sited in a way that is protected from accidental and environmental threats and always connected with adequate supporting utilities both if inside the organisation premises or outside them.
10	**Malware protection**	12.2.1	Malware protection software should be installed and kept constantly up-to-date on all assets that can be infected by malware.
11	**Information security procedures**	12.1.1	Information security procedures should be applied, documented, maintained, and be available to all users.
12	**Software vulnerability patching**	12.5.1 12.6.1	Security patches made available by vendors to overcome software vulnerabilities should be constantly evaluated and timely installed on all systems. *Suggested patching frequency: monthly*
13	**Network security**	13.1.1 13.1.2	ICT networks should be designed to limit the possibility for eavesdropping or altering the traffic, additionally limiting the authorised communications to the necessary ones while blocking all the others.
14	**Security in supplier agreements**	15.1.1 15.1.2 15.1.3	All suppliers with whom information are exchanged should be aware of the organisation's applicable security policies and be contractually bound to respect them, allowing verifications to be performed. This approach should also extend to their sub-contractors.
15	**Incident analysis and response**	16.1.2 16.1.3 16.1.4 16.1.5	All information systems and services users should note and report any observed or suspected security weaknesses for analysis. Specific incident response procedures should be activated depending on the analysis outcomes, while keeping full traceability of the evolving situation.
16	**Identification of legislation and contractual requirements**	18.1.1 18.1.4	All applicable information security requirements deriving from national, international or sectorial legislation should be kept under constant control as the ones deriving from contracts with third parties, with specific attention to personal data protection.

A.2 Discretionary controls

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
01	**External contacts and communications management**	6.1.3 6.1.4	The organisation should develop sufficient contacts with the authorities in order to swiftly react to widespread threats and with special interest groups, forums or associations mainly in order to get actual threat and control information.
02	**Remote working**	6.2.2	Remote working tools should be developed considering additional security protection to avoid information leaks and misuse. Remote accesses used for this purpose should be strengthened against unauthorised access
03	**Mobile device management**	6.2.1	Mobile devices used for working purposes should be securely configured and strictly controlled.
04	**Personnel screening**	7.1.1	All employees and third-party personnel regularly accessing the organisation's premises should have their criminal history and relevant background screened in accordance with relevant laws, regulations and ethics. The screening should be proportional to the business requirements.
05	**Personnel contract clauses**	7.1.2 7.2.3 7.3.1 13.2.4	All employees and third-party personnel should sign non-disclosure agreements before having any interaction with the organisation's information and their contract should require the respect of the organisation's information security policies. Consequences for disregarding those mandates, including after position changes or termination, should also be clearly defined.
06	**Removable media management**	8.3.1 8.3.3 13.2.1 13.2.2 18.1.3	Specific handling restrictions should be defined and implemented for all removable and portable media. Media containing information should be protected against unauthorised access misuse or destruction in case of transfer outside of the organisation's premises.
07	**Information disposal**	8.3.2 11.2.7	Strict procedures should be applied for the secure and safe disposal of media to be reassigned or dismissed in order to render previously stored data unrecoverable. *Suggested information disposal: full overwrite*
08	**Access control policy**	9.1.1 9.1.2	A formal access control policy covering the organisation's system and networks should be documented, maintained and reviewed in accordance with the security requirements, information classification and management and personnel authorisation levels.
09	**Encryption**	10.1.1 10.1.2	Cryptographic controls using strong algorithms should be developed, documented, implemented, maintained and reviewed to ensure confidentiality of confidential information transmitted and at rest. Cryptographic keys should be used, protected and kept according to strict and documented procedures during their whole lifecycle. *Suggested encryption algorithms: AES128+, SHA512+, RSA2048+*
10	**Physical security**	11.1.1 11.1.2 11.1.3 11.1.6	Physical protected barriers and secure areas to minimise unauthorised access to the organisation's premises and its information systems should be defined and equipped with access controls systems. Access points, including the ones for loading and unloading, should be minimised and equally secured.

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
11	**Environmental threats protection**	11.1.4	Physical protection against damages from natural causes or any other kind of natural or man-made disaster should be designed and applied to premises and information systems within them, starting from fire, humidity and earthquake protections. *Suggested threats to consider: fire, humidity, earthquake*
12	**Equipment maintenance**	11.2.4	All items of equipment should be maintained in the context of the Information Security Plan of the organisation. Maintenance access to information systems should be controlled.
13	**Unattended workplace and equipment**	11.2.8 11.2.9	Unattended equipment should be always left with the appropriate protection against physical unauthorised access and theft. All sessions should be locked when leaving any equipment and disconnect automatically after a defined inactivity period. No media should be left unattended in a workplace. *Suggested session timeout/screen saver: 15 minutes*
14	**Change management**	12.1.2 12.6.2 14.2.2 14.2.4	All changes to the organisation, business and information processes or systems that affect information security should be registered, duly approved and tested. System and software modifications should be allowed only to authorised personnel.
15	**Separation of development and test environments**	12.1.4 14.3.1	Development, test and operational facilities should be as much separated as possible to reduce the risks of unauthorised access or changes to the operational system. Data used for development and testing should additionally be different from production ones (anonymised or not related to real persons/facts). *Suggested separation: different systems and networks*
16	**Backup**	12.3.1	Backup copies of information and software should be created and tested regularly in accordance with a defined backup policy. *Suggested backup frequency: daily/weekly*
17	**Event logging and storage**	12.4.1 12.4.2 12.4.3	Event logging records of most security-relevant operations should be produced, securely stored, protected from both access and modifications and regularly reviewed. All system administrator and system operator activities should be logged as succeeded and attempted login/logouts. *Suggested log retention: 6 months+*
18	**Time synchronisation**	12.4.4	System clocks should be constantly synchronised in all areas of the organisation or in a security domain with an agreed and reliably accurate time source.
19	**Network segregation**	13.1.3	Information services, users, and information systems should be segregated within different network areas with homogeneous security requirements. The segregation should be performed using firewalls or equivalent devices.
20	**Messaging security**	13.2.3	Information transferred via electronic messaging and the supporting systems should ensure confidentiality and detect attacks through these channels.
21	**Security by design**	6.1.4 14.1.1	Information security should represent an integral part of information systems across their entire lifetime, starting from the requirements for

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
		14.2.5	information systems early design. All the organisation's projects should include information security considerations as early as possible.
22	**Application services security**	14.1.2 14.1.3	Information systems used to provide services should be protected against common attacks through a secure and hardened configuration, developed to use additional security controls and constantly monitored/protected through security dedicated devices proportionally to their exposure. *Suggested security devices: firewalls and IDS/IPS*
23	**Secure development lifecycle**	14.2.1 14.2.6 14.2.7	Organisations should establish secure development lifecycle criteria for their applications, to be applied also for external custom projects in order to minimise applications' vulnerabilities.
24	**Security testing**	14.2.3 14.2.8 14.2.9 18.2.3	Security and acceptance criteria for new information systems, upgrades and new versions should be established and suitable tests of the system carried out during development, prior to acceptance and periodically thereafter, requiring previous fixing of discovered vulnerabilities. *Suggested periodicity: every 6 months internal, every quarter external*
25	**Suppliers security monitoring**	15.2.1 15.2.2	The implementation of changes to supplier services should be monitored, controlled and reviewed by the use of formal change control procedures. The respect of security clauses and security service levels should be constantly monitored.
26	**Incident management policy**	16.1.1	Information security incidents should be controlled, registered, handled and addressed according to specific responsibilities approved and established by the management. Appropriate communication and escalation procedures should also be established.
27	**Incident lesson learned**	16.1.6	Knowledge gained from analysing and resolving information security incidences should be used to reduce the likelihood or impact of future incidents possibly adapting incident response procedures.
28	**Redundancy management**	17.2.1	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements also in failure situations.
29	**Intellectual property protection**	18.1.2	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material covered by intellectual property rights and on the use of proprietary software products.
30	**Information security assessments and audits**	18.2.1 18.2.2	Information security systems should be regularly reviewed by independent auditors. Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. Information systems should be regularly reviewed to provide continuous compliance with security implementation standards.

A.3 Discretionary controls threat relationship (mitigation)

ID	Control	Physical attack	Unintentional damage	Disaster	Failures-malfunction	Outages	Eavesdropping-interception-hijacking	Legal	Nefarious-activity-abuse
A2.01	External contacts and communications management	Secondary		Primary		Secondary	Primary		Secondary
A2.02	Remote working			Secondary		Secondary	Primary		
A2.03	Mobile device management	Secondary	Secondary	Secondary		Secondary	Primary		Secondary
A2.04	Personnel screening				Secondary		Primary	Primary	Secondary
A2.05	Personnel contract clauses	Secondary	Secondary		Secondary		Primary	Primary	Primary
A2.06	Removable media management	Primary	Primary	Secondary	Secondary	Secondary	Primary	Secondary	
A2.07	Information disposal	Secondary	Secondary		Secondary		Primary		
A2.08	Access control policy						Primary		Primary
A2.09	Encryption						Primary	Primary	
A2.10	Physical security	Primary	Secondary				Primary		
A2.11	Environmental threats protection	Primary	Secondary	Primary		Primary	Secondary		
A2.12	Equipment maintenance	Primary	Primary		Primary	Secondary			
A2.13	Unattended workplace and equipment	Secondary					Primary		
A.2.14	Change management		Secondary		Secondary		Primary		Secondary
A.2.15	Separation of development and test environments				Secondary		Secondary		
A.2.16	Backup	Primary	Primary	Primary	Primary	Secondary		Secondary	Secondary
A.2.17	Event logging and storage		Secondary		Secondary		Primary	Secondary	Primary
A.2.18	Time synchronisation		Secondary		Secondary		Primary	Secondary	Primary

ID	Control	Physical attack	Unintentional damage	Disaster	Failures-malfunction	Outages	Eavesdropping-interception-hijacking	Legal	Nefarious-activity-abuse
A.2.19	Network segregation		Secondary			Secondary	Primary		Secondary
A.2.20	Messaging security		Secondary				Primary	Secondary	Secondary
A.2.21	Security by design		Secondary		Secondary	Secondary	Primary		Primary
A.2.22	Application services security		Secondary				Primary	Secondary	Primary
A.2.23	Secure development lifecycle		Primary				Primary		Secondary
A.2.24	Security testing		Secondary				Primary		Primary
A.2.25	Suppliers security monitoring				Secondary	Primary		Secondary	
A.2.26	Incident management policy	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary
A.2.27	Incident lesson learned	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary
A.2.28	Redundancy management			Primary	Primary	Primary		Secondary	Primary
A.2.29	Intellectual property protection							Primary	
A.2.30	Information security assessments and audits		Secondary				Secondary	Primary	Secondary

Annexe X

Politique de sécurité de l'information					
Politique nº:		**Date de prise d'effet:**		**Courriel:**	
Version:		**Contact:**		**Téléphone:**	

Objet

The information security policy, related policies and procedures of the company are intended to protect the confidentiality, integrity and availability (CIA) of all the organisation's critical data and assets according to its business interests.

Champ d'application

Cette politique s'applique aux employés, contractants, consultants, travailleurs (temporaires et autres) de l'entreprise, y compris à l'ensemble du personnel affilié à des tierces parties. Elle s'applique à tous les actifs, matériels et immatériels, qui appartiennent à l'entreprise ou sont utilisés par l'entreprise.

Politique

La direction de l'entreprise considère que la sécurité de l'information fait partie des principaux facteurs clés de son activité et s'emploie activement à promouvoir et à financer toutes les initiatives permettant de réduire à moindre coût les risques liés à la sécurité de l'information, de garantir la conformité aux exigences légales et contractuelles, et de respecter les bonnes pratiques sectorielles.

L'ensemble du personnel interne et externe de l'entreprise doit respecter scrupuleusement l'intention et les prescriptions de la présente politique et de toutes les politiques et procédures connexes pour éviter de s'exposer à des sanctions disciplinaires. Plus spécifiquement, les principes de la sécurité de l'information qui doivent être compris et observés par chacun sont :

1) La sécurité de l'information n'est pas absolue, elle doit toujours être proportionnée aux risques qu'elle doit prévenir;
2) Tous les accès doivent être strictement liés à la nécessité de connaître le personnel et les besoins de son travail;
3) Les ressources doivent être réparties et protégées selon leurs exigences de sécurité de l'information;
4) Il est toujours préférable d'utiliser des normes et des solutions ouvertes et non des choix propriétaires et obscurs;
5) Dans certains cas, une unique couche de contrôles de sécurité de l'information peut ne pas suffire parce que les contrôles peuvent échouer: en cas de risque de panne grave, il est possible d'utiliser des approches à couches multiples;
6) Il est indispensable d'étudier, de pratiquer et de tester les situations pertinentes pour la sécurité de l'information pour s'assurer d'être prêt à y répondre efficacement;
7) La sécurité de l'information est la responsabilité et le devoir de chacun ; ce n'est pas le problème des autres.

L'entreprise définit et mesure un ensemble d'objectifs de sécurité de l'information spécifiques, qui sont constamment contrôlés et améliorés. Ces objectifs doivent orienter en permanence les décisions tactiques en matière de sécurité de l'information, tout comme les principes ci-dessus mentionnés guident les décisions stratégiques.

L'amélioration continue est d'une importance capitale pour tenir à distance les risques de plus en plus importants liés à la sécurité de l'information et permettre à l'entreprise d'atteindre ses objectifs commerciaux dans l'environnement complexe dans lequel elle évolue aujourd'hui.

Approbation et propriété

Propriétaire	Titre	Date	Signature
Auteur de la politique	Titre	JJ/MM/AA	
Approuvé par	**Titre**	**Date**	**Signature**
Équipe de gestion	Titre	JJ/MM/AA	

European Commission

EFTA AELE

Small Business Standards

European DIGITAL SME Alliance

Cofinancé par la Commission européenne et l'AELE

sbs-sme.eu
@SBS_SME

digitalsme.eu
@EUdigitalsme