Small Business Standards

Guide pour PME en matière de Contrôles de sécurité de l'information

European DIGITAL SME Alliance

Ce guide a été élaboré par un groupe ad hoc créé par des experts du groupe de travail Digitalisation de SBS et des groupes de travail Normalisation, Cybersécurité, et Protection des Données de DIGITAL SME. Le groupe ad hoc était composé d'experts en normalisation familiers avec les questions de cybersécurité qui comprennent parfaitement les besoins des PME dans ce milieu.

Président :
Jean-Luc Allard

Coordinateur :
Omar Dhaher

Experts :

Andrea Caccia Daniele

Tumietto

Davide Giribaldi

Francisco Menéndez

Samuel Fricker

Publication :
Mars 2022

À PROPOS DE CE GUIDE

Small Business Standards (SBS) est l'association qui représente les intérêts des petites et moyennes entreprises (PME) européennes en matière de normalisation aux niveaux européen et international. Ses principaux objectifs sont dérivés du règlement 1025/2012 sur la normalisation européenne. SBS vise à accroître la sensibilisation et l'influence des PME en matière de normalisation. Pour ce faire, elle facilite l'adoption de normes par les PME, représente leurs intérêts et les motive à s'engager dans le processus de normalisation.

European DIGITAL SME Alliance (DIGITAL SME) est membre de SBS. Il s'agit du plus grand réseau de PME du continent travaillant dans le domaine des TIC, représentant environ 45 000 PME numériques.

Dans ses efforts pour sensibiliser et aider les PME à adopter et à utiliser les normes de cybersécurité, SBS a publié un guide PME sur l'ISO/CEI 27001 en 2017. Reconnaissant la nécessité croissante pour les PME de respecter les exigences en matière de cybersécurité et de renforcer leurs capacités techniques à cet égard, SBS a élaboré ce guide sur la norme ISO/CEI 27002 sur le contrôle de la sécurité de l'information pour les PME.

SBS est l'unique propriétaire de ce guide gratuit et accessible au public.

Liste des acronymes

AVPA : Apportez votre propre appareil

PDG : Directeur général

CERT: Équipe d'intervention d'urgence informatique

COBIT : Objectifs de contrôle des technologies de l'information et des technologies connexes (ISACA.org)

DAC : Contrôle d'accès discrétionnaire

DTG: Groupe date-heure

DPO : Délégué à la protection des données

EGIT : Gouvernance de l'information et de la technologie d'entreprise

RGPD : Règlement général sur la protection des données

EIC : Commission électrotechnique internationale

TIC : Technologies de l'information et des communications

IoT : Internet des objets

IP : Protocole Internet

SMSI : Système de management de la sécurité de l'information

RSI : Responsable de la sécurité de l'information

ISO : Organisation internationale de normalisation

LAN : Réseau local

MAC : Contrôle d'accès obligatoire

OS : Système d'exploitation

ICP : Informations à caractère personnel

PIMS : Système de management des ICP

RACI : RACI est une matrice d'affectation de gestion. L'acronyme signifie :

Responsables, les personnes qui sont en charge de faire le travail ;
Redevable, la personne qui est ultimement responsable d'atteindre les objectifs et qui relève de la haute direction ;
Consultées, les personnes dont les conseils sont recherchés pour sélectionner les objectifs et définir les activités, et ;
Informées, les personnes qui devraient être mises au courant des activités et des résultats attendus.

VPN : Réseau privé virtuel

WAN : Réseau étendu

TABLE MATIERES

1 INTRODUCTION 6

2. CHAMP D'APPLICATION 7

3 DÉFINITIONS 8

3.1 Définitions générales 8
3.2 Définitions de la protection des renseignements personnel 9
3.3 Définitions relatives à la sécurité 10

4 POURQUOI LES PME DOIVENT-ELLES PROTÉGER L'INFORMATION ? 11

4.1 Différences entre la sécurité de l'information et celle des TIC 14
4.2 Influence d'Internet et aspects cyber 14

5 PROTECTION DE LA VIE PRIVÉE 15

5.1 Principaux concepts 15
5.2 Attestations liées à la protection des données personnelles 15
5.3 Contrôles concernant la protection de la vie privée 17

6 GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION 18

6.1 Qu'est-ce que la gouvernance de la sécurité de l'information? 18
6.2 ISO/CEI 27014 19
6.3 COBIT 19

7 CONTRÔLES DE LA SÉCURITÉ DE L'INFORMATION ET DE LA PROTECTION DE LA VIE PRIVÉE 21

7.1 Introduction 21
7.2 Contrôle 23

8 CONTRÔLE #1 : GESTION DES ACTIFS 24

10 CONTRÔLE # 2 : POLITIQUES, NORMES ET LIGNES DIRECTRICES 27

11 CONTRÔLE #3 : GESTION DES INCIDENTS 29

12 CONTRÔLE #4 : GESTION DU CONTRÔLE D'ACCÈS 32

13 CONTRÔLE #5 : SÉCURITÉ DU RÉSEAU ET ÉCHANGES DE DONNÉES 35

14 CONTRÔLE #6 : GESTION DES VULNÉRABILITÉS 38

15 CONTRÔLE #7 : LUTTE CONTRE LES LOGICIELS MALVEILLANTS 40

16 CONTRÔLE #8 : GESTION DES BACKUPS 41

17 CONTRÔLE #9 : GESTION DES MESURES DE PROTECTION 43

18 CONTRÔLE #10 : PRÉPARATION DES TIC À LA CONTINUITÉ DES ACTIVITÉS 45

19 CONTRÔLE #11 : TÉLÉTRAVAIL 51

20 CONTRÔLE #12 : SURVEILLANCE DES CYBERMENACES 53

21 CONTRÔLE #13 : SENSIBILISATION À LA SÉCURITÉ DE L'INFORMATION 55

22 CONTRÔLE #14 : ASPECTS PORTANT SUR LA SÉCURITÉ DE L'INFORMATION DANS LES RELATIONS AVEC LES FOURNISSEURS 57

23 CONTRÔLE #15 : ORGANISATION DE LA SÉCURITÉ DE L'INFORMATION 60

24 CONTRÔLE #16 CONTRÔLES SUPPLÉMENTAIRES DE PROTECTION DE LA VIE PRIVÉE 64

25 CONCLUSION 69

1 ANNEXE A : TECHNIQUE DE CLASSIFICATION DE L'INFORMATION 71

1.1 Introduction 71
1.2 Procédure 71

2 ANNEXE B : LISTE DES TITRES DE CONTRÔLE AVEC LEUR NUMERO, PAR REFERENCE 80

3 ANNEXE C : PROCESSUS COBIT ET GESTION DE LA SÉCURITÉ 83
4 ANNEXE D : LISTE DES ÉQUIPES D'INTERVENTION D'URGENCE INFORMATISÉES 87
5 RÉFÉRENCES 88
6 À PROPOS DES EXPERTS 90

1 INTRODUCTION

La transformation numérique joue un rôle important dans la restructuration des entreprises à travers le monde. Les technologies habilitantes comme la 5G, l'intelligence artificielle, la blockchain, l'informatique de pointe et l'Internet des objets (IoT) sont au cœur de cette transformation. Reconnaissant son rôle stratégique pour les objectifs à long terme de l'UE, la Commission européenne a élaboré sa Stratégie 2030 — la Décennie DIGITALE — qui comprend les objectifs suivants :

1. 75 % des entreprises européennes devront adopter les services informatiques du Cloud, le big data et l'intelligence artificielle ;
2. Plus de 90 % des PME européennes atteindront au moins un niveau basique d'intensité numérique ;
3. Augmenter le nombre de mises à l'échelle et de financements pour doubler le nombre de licornes européennes.

Les PME numériques fournissent des solutions innovantes dans des domaines tels que la 5G, l'IoT, l'informatique de pointe, pour permettre à d'autres entreprises d'atteindre les compétences numériques et de réaliser la transformation numérique. Dans ce cadre de travail, la sécurité reste un élément crucial à adopter pour résoudre les besoins des technologies et les solutions pour les entreprises.

La cybersécurité est une exigence de l'ensemble de la chaîne d'approvisionnement pour assurer une transformation en douceur des processus industriels, de l'espace physique au cyberespace[1]. Puisque 99 % des entreprises européennes sont des PME, la protection contre les cyberattaques devient cruciale pour l'économie européenne.

Cependant, l'adoption des TIC et de la sécurité de l'information est faible. En 2019, Eurostat a estimé que 33 % des entreprises de l'UE disposent de documents sur les mesures, pratiques ou procédures relatives à la sécurité des TIC, tandis que 24 % des entreprises de l'UE ont défini ou examiné les documents de sécurité

[1] SBS (2020, page 3), Loi européenne sur la cybersécurité et le rôle des normes pour les PME

des TIC au cours des 12 derniers mois.

Les normes de cybersécurité peuvent aider les entreprises à respecter un ensemble d'exigences qui fournissent une protection de base nécessaire. Toutefois, la mise en œuvre de ces exigences demeure complexe et coûteuse pour les PME. En 2020[2], il y avait environ 32 000 certificats ISO/CEI 27001, Système de management de la sécurité de l'information, dans le monde entier, alors qu'il y a environ 190 millions d'entreprises opérant dans le monde.

Le guide est rédigé par des propriétaires de PME et des professionnels qui travaillent dans ou pour des PME ayant accumulé de l'expérience et des connaissances sur les défis en matière de sécurité auxquels la plupart des petites entreprises font face quotidiennement. Il est composé de deux parties principales. La première partie explique la nécessité d'une stratégie et d'objectifs clairs pour une mise en œuvre efficace des contrôles de sécurité et introduit les concepts de base de la vie privée et leur pertinence pour les contrôles de sécurité, les certifications et la conformité au RGPD. La deuxième partie recommande les contrôles essentiels minimaux que les PME doivent mettre en œuvre pour protéger leurs informations et se conformer aux règles du RGPD.

2. CHAMP D'APPLICATION

Le présent guide porte sur la sécurité de l'information au sens le plus large. Le guide s'adresse à la fois à la direction des PME (CEO et DPO) et aux équipes techniques (fournisseurs de cybersécurité des PME, praticiens/experts en cybersécurité) et aux PME travaillant directement dans le digital. Pour la direction des PME, le guide vise à sensibiliser aux problèmes auxquels sont confrontées les PME et à les aider à prendre les devants dans les activités que leur personnel technique ou leurs fournisseurs de sécurité devraient mener. Le guide sensibilise le lecteur aux questions liées à :

- L'Importance de protéger les informations (article 4)
- La protection de la vie privée et respect du RGPD (section 5)
- La gouvernance de la sécurité de l'information (section 6)
- Les contrôles de sécurité de l'information (section 7.1)

La gestion des risques liés à la sécurité de l'information n'est pas abordée directement, car il ne s'agit pas d'un contrôle. Ce sujet est traité dans le Guide PME SBS pour la mise en œuvre de la norme ISO/CEI 27001 sur le management de la sécurité de l'information.

Les PME disposant de compétences et de connaissances adéquates[3] en matière de cybersécurité peuvent alors passer à la section 7.2, qui fournit un aperçu des 16 contrôles sélectionnés, jugés essentiels pour toute PME afin de protéger ses informations et de se conformer aux règles du RGPD. Le guide vise à appuyer la transformation des PME qui souhaitent prendre conscience de « la cybersécurité et des pratiques de cybersécurité appropriées ». Les équipes techniques et les experts en cybersécurité peuvent consulter les contrôles présentés à la section 7 pour assurer la mise en œuvre optimale des mesures de sécurité pour l'infrastructure des PME.

Il est fortement conseillé aux PME, y compris les microentreprises qui n'ont pas de DPO ou de professionnels de la sécurité dédié, de demander l'aide de PME et/ou de praticiens de la cybersécurité pour assurer une

[2] SBS (2020, page 4), EU Cybersecurity Act and the role of standards for SMEs

[3] Shojaifar et Järvinen (2021, page 3), une PME qui fait partie des colonnes (ACCS et RPG) pourrait poursuivre avec la section 7.2. D'autres PME ont besoin de l'aide d'autres PME ou professionnels de la cybersécurité pour mettre en œuvre les contrôles énoncés à la section 7.2. Cliquez ici pour plus d'informations sur le cadre théorique développé par Shojaifar et Järvinen.

protection adéquate de leurs données.

3 DÉFINITIONS

3.1 Définitions générales

Continuité d'activité (BC) : Désigne les activités de maintien des fonctions opérationnelles de base de l'ensemble de l'organisation ou leur reprise rapide en cas de perturbation, comme une attaque de cybercriminels.

Plan de continuité d'activité : Ensemble de procédures et d'instructions qu'une organisation doit suivre pour réagir rapidement à un incident. Un plan de continuité des activités couvre les processus opérationnels, les actifs, les ressources humaines, les partenaires commerciaux et toutes les parties prenantes impliquées dans l'écosystème de l'entreprise.

Analyse des répercussions sur les activités : Il s'agit d'un autre élément essentiel d'un plan de BC. Il identifie l'impact des pertes d'affaires (généralement quantifiées en coûts) et aide à examiner l'ensemble des processus de l'organisation et à les évaluer, en déterminant lesquels sont les plus importants.

Contrôle : Mesure (processus, politique, dispositif, pratique ou action) qui modifie le risque.

Confidentialité : Propriété que l'information n'est pas mise à disposition ou divulguée à des personnes,

entités ou processus non autorisés.

Plan de reprise après sinistre : Un élément important d'un plan de BC, mais qui n'est pas le plan lui-même. Il se concentre principalement sur la restauration d'une infrastructure informatique et toutes les opérations connexes après un incident.

Gouvernance de la sécurité de l'information : Système par lequel les activités de sécurité de l'information d'une organisation sont dirigées et contrôlées.

Sécurité de l'information : Préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information.

Risque lié à la sécurité de l'information : Le risque lié à la sécurité de l'information est associé à la potentialité que les menaces exploitent les vulnérabilités d'un (ou d'un groupe de) bien(s) informationnel(s) et causent ainsi un dommage à une organisation.

Système d'information : Ensemble d'applications, de services, d'actifs de technologie de l'information ou d'autres composants de traitement de l'information.

Intégrité : Propriété d'exactitude et d'exhaustivité.

Politique : Intentions et orientations d'une organisation, telles qu'exprimées formellement par sa haute direction.

Processus : Ensemble d'activités interdépendantes ou en interaction qui transforme les entrées en sorties.

Gestion des risques : activités coordonnées pour diriger et contrôler une organisation en matière de risques.

3.2 Définitions de la protection des renseignements personnel

Les définitions suivantes sont conformes au RGPD. La norme ISO/CEI 27701 et, en général, les normes ISO utilisent le terme « informations personnelles identifiables (IPI) » alors que le terme « données personnelles » est utilisé dans le RGPD. Par conséquent, le guide utilisera le terme « données personnelles ».
Données personnelles : Toute information relative à une personne physique identifiée ou identifiable.

Personne concernée : Personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques au physique ou à l'identité physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne.

Traitement des données à caractère personnel : toute opération ou ensemble d'opérations effectuées sur des (ensembles de) données à caractère personnel, par des moyens automatisés ou non, tels que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, la recherche, la consultation, l'utilisation, la divulgation par transmission, diffusion ou autre mise à disposition, l'alignement ou combinaison, la restriction, l'effacement ou la destruction.

Responsable du traitement : Personne physique ou morale, autorité publique, organisme ou autre organisme qui, seul ou conjointement avec d'autres, détermine les fins et les moyens du traitement des données à caractère personnel ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou d'un État membre, le responsable du traitement ou les critères spécifiques pour sa

désignation peuvent être prévus par le droit de l'Union ou de l'État membre.

Sous-traitant : Personne physique ou morale, autorité publique, agence ou autre organisme qui traitent des données à caractère personnel pour le compte du responsable du traitement.

3.3 Définitions relatives à la sécurité

Disponibilité : Propriété d'être accessible et utilisable sur demande par une entité autorisée.

Confidentialité : Propriété que l'information n'est pas mise à la disposition ou divulguée à des personnes, entités ou processus non autorisés.

Information documentée [4]: Information devant être contrôlée et maintenue par une organisation ainsi que le support sur lequel elle est contenue.

Événement lié à la sécurité de l'information : Occurrence d'un état de système, de service ou de réseau indiquant une violation possible de la politique de sécurité de l'information ou une défaillance des contrôles, ou une situation auparavant inconnue qui peut être pertinente sur le plan de la sécurité.

Incident lié à la sécurité de l'information : événement unique ou série d'événements indésirables ou imprévus de sécurité de l'information qui ont une probabilité importante de compromettre les activités

[4] L'information documentée peut être dans n'importe quels format et média et de n'importe quelle source. L'information documentée peut faire référence au système de management, y compris les processus connexes, ou l'information créée pour que l'organisation puisse fonctionner (documentation) et la preuve des résultats obtenus (dossiers).

commerciales et de menacer la sécurité de l'information.

Potentialité : Possibilité que quelque chose se produise.

Logiciels malveillants : Il existe un large éventail de types de logiciels malveillants :

Virus : Se réplique dans des fichiers exécutables.

Ver : Voyage à travers les canaux de communication via les contacts de l'utilisateur.

Spyware : Surveille vos activités et envoie des informations au serveur d'un pirate.

Ransomware : Gèle votre système en cryptant les fichiers et le pirate promet de vous rendre accès après avoir payé une rançon.

Bombe logique : Repose silencieusement dans votre système jusqu'à ce que des conditions spécifiquement programmées se produisent, puis il éclate causant des dommages irréversibles.

Cheval de Troie : Inclus dans un logiciel bénin que vous avez acheté ou téléchargé, et qui effectue plusieurs activités cachées.

Vulnérabilité : Faiblesse d'un actif ou d'un contrôle qui peut être exploitée par une ou plusieurs menaces.

4 POURQUOI LES PME DOIVENT-ELLES PROTÉGER L'INFORMATION ?

L'information est probablement l'atout le plus important pour toute organisation, y compris les PME. Que peut faire une organisation si l'information n'est pas fiable ou est déjà entre les mains d'une personne qui peut vous bloquer ou modifier des données sans que vous le sachiez ? Ou, simplement, que faire si l'information n'est pas disponible ou accessible lorsque vous en avez besoin ? Toute l'information accessible sur Internet est-elle fiable ?

La plupart d'entre nous connaissent ISO 9001, le fameux système de management de la qualité. Connaissez-vous l'existence de la norme ISO/CEI 27001 qui traite du système de management de la sécurité de l'information ? Sa première publication remonte à 2005 et sa structure et son contenu sont très similaires à ISO 9001. Si vous avez mis en œuvre la première norme, vous pouvez mettre en œuvre la deuxième sans trop d'effort. Se référer donc au «Guide PME SBS pour la mise en œuvre de la norme ISO/IEC 27001 sur le management de la sécurité de l'information».

Cependant, il faut comprendre la portée et le besoin de cette information. Qu'est-ce que l'information ? Pourquoi devons-nous la protéger ? Quel est le lien avec le RGPD ? Ce sont les questions auxquelles le présent guide vise à répondre.

Qu'est-ce que l'information ?

L'information est un ensemble de données interprétables qui, dans un contexte donné, a (ont) une signification et une valeur. Pour assurer et améliorer la valeur de ces données, l'interopérabilité et le contexte doivent être préservés et protégés.

Pourquoi ? Simplement parce que, sans information et plus spécifiquement sans information fiable, très peu est réalisable dans notre vie. Les êtres humains — et encore plus naturellement et inconsciemment notre corps — ne font rien d'autre que de manipuler des données et des informations en permanence : par exemple, préparer du pain, conduire une voiture et guérir un problème physique. L'information est étroitement liée à toute activité humaine.

L'information est essentielle, car elle sert à :

- accroître nos connaissances et nos compétences (nous savons tous que les connaissances nous donnent le pouvoir[5] sur ceux qui ne l'ont pas) ;
- prendre de bonnes décisions ;
- agir pour atteindre nos objectifs ;
- mesurer nos réalisations.

Qu'arrive-t-il si les informations utilisées ne sont pas fiables parce qu'elles sont :

- déjà entre les mains de ceux qui peuvent nous empêcher d'atteindre nos objectifs (confidentialité) ?
- modifiées de manière incontrôlée dans l'une des phases de sa manipulation (intégrité) ?
- indisponibles et inaccessibles lorsque nous en avons besoin (disponibilité) ?

[5] Pouvoir 1 : De celui qui connaît sur les ignorants ; Pouvoir 2 : Connaître quelqu'un d'autre et l'utiliser pour obtenir quelque chose (chantage) ; Pouvoir 3 : Empêcher d'accéder à l'information nécessaire (désactiver la personne).

Qu'est-ce que la sécurité de l'information ?

La confidentialité, l'intégrité et la disponibilité sont depuis longtemps les trois principaux critères de sécurité de l'information. Le respect des lois et réglementations, où le traitement des données à caractère personnel est certainement l'une des questions les plus pertinentes à traiter, devient de plus en plus une priorité pour les PME, ne serait-ce qu'en raison des sanctions encourues.

Les deux normes « clés » en matière de sécurité de l'information sont ISO/CEI 27001 (Système de management de la sécurité de l'information – SMSI) et ISO/CEI 27002 (Code de bonnes pratiques en matière de contrôles de sécurité de l'information). L'application de la norme ISO/CEI 27001 sur les données à caractère personnel (DCP) améliore également directement le niveau de conformité au Règlement général sur la protection des données (RGPD), bien qu'elle ne le garantisse pas directement, mais il existe maintenant la norme ISO/CEI 27701, une norme spécifique traitant de cette question.

Cependant, une gestion sophistiquée de l'information utilisée est nécessaire. ISO/CEI 27002 est une liste de 114 contrôles pour assurer la sécurité de l'information. Ceux-ci sont généralement déterminés, en particulier pour leur mise en œuvre dans chaque contexte, dans le cadre d'un processus de gestion des risques comme expliqué dans la norme ISO/CEI 27005.

Le RGPD exige une gestion contrôlée des DCP, qui sont une des catégories d'information traitée par une PME : celles-ci concernent leur personnel, leurs clients et leurs fournisseurs dès que le nom d'une personne est associé à autre chose. Les normes ISO/CEI 27001 et 27002 sont également applicables et sont complétées par la norme ISO/CEI 27701.

Le processus d'évaluation des risques pour la sécurité de l'information identifie également les risques liés au traitement des données à caractère personnel et, en particulier, à la perte de confidentialité, d'intégrité et de disponibilité de ces données. Les contrôles et les autres recommandations du présent guide visent à réduire les risques évalués. De plus amples renseignements sur le processus de gestion des risques se trouvent dans le Guide des PME pour la mise en œuvre de la norme ISO/CEI 27001 sur le management de la sécurité de l'information.

Pourquoi avons-nous besoin de normes pour cela ?

Les lois et réglementations européennes récentes et à venir s'appuient systématiquement sur le principe de responsabilité et une approche fondée sur le risque, en particulier pour les nouvelles technologies qui sont particulièrement pertinentes pour les start-ups. La complexité et le coût de la conformité sans une approche structurée cohérente peuvent rapidement devenir ingérables pour toute organisation et les normes représentent une solution reconnue pour y remédier.

Quiconque parle la langue de la société dans laquelle il/elle vit utilise deux normes de facto pour comprendre les situations et être compris : l'orthographe et la grammaire. Ainsi, les normes de sécurité de l'information nous aident à mieux mettre en œuvre les actions conformément à la réglementation, à gérer la situation unique de chaque entité et à accroître la compétitivité.

Les normes de sécurité de l'information relèvent du sous-comité 27 du Comité technique mixte 1 au sein de l'ISO et du CEI (Comité électrotechnique international), connus sous le nom de l'ISO/CEI JTC 1 SC 27 : Sécurité de l'information, cybersécurité et protection de la vie privée.

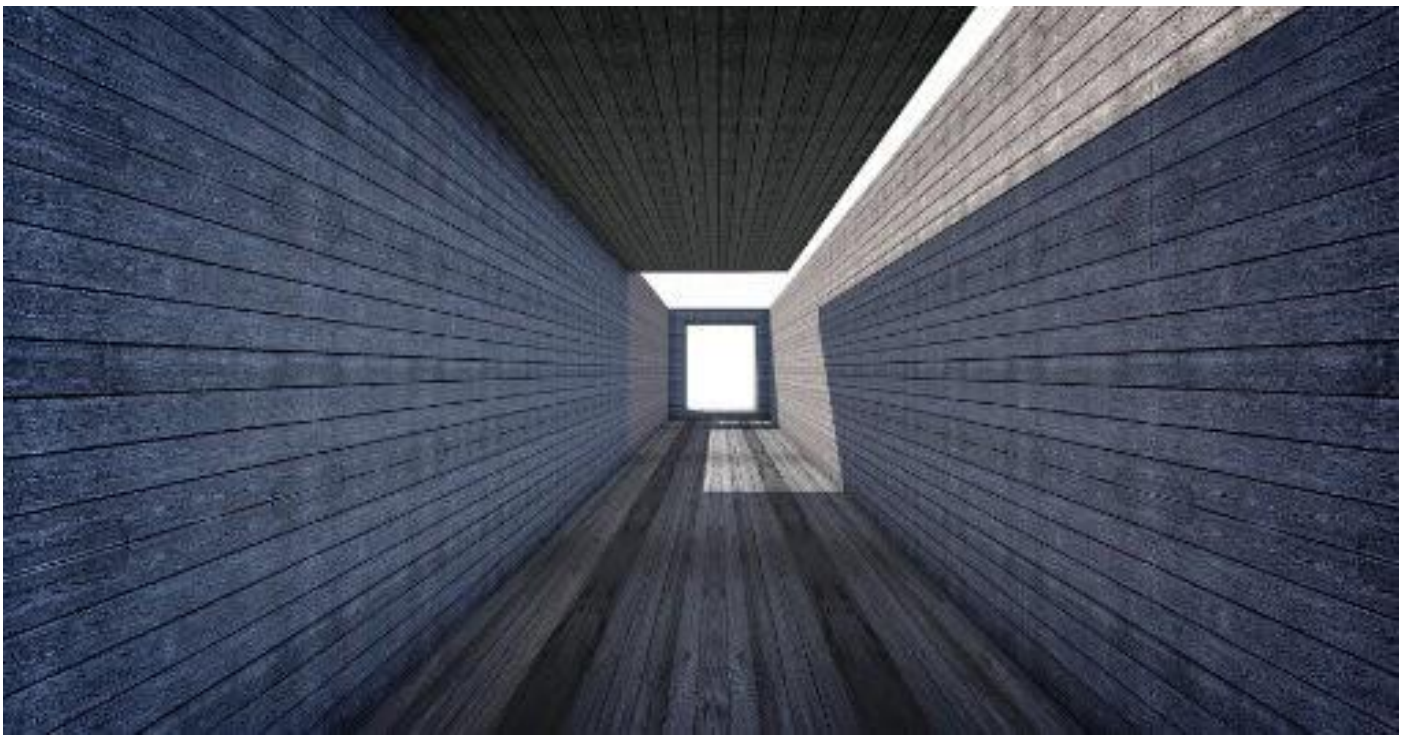
Les normes sont élaborées pour les entreprises de toutes tailles. Cependant, l'identification de celles qui conviennent et leur adaptation, en particulier pour les PME, peuvent constituer un obstacle à leur utilisation. Ce document se veut un guide pour la sélection et l'adaptation des normes dans ce domaine pour les PME.

4.1 Différences entre la sécurité de l'information et celle des TIC

La sécurité de l'information concerne la protection de l'information, quel que soit le support (physique, parlé ou projeté, et sur les médias et systèmes numériques). La sécurité des TIC concerne la protection des systèmes TIC et des données qu'ils contiennent et traitent.

4.2 Influence d'Internet et aspects cyber

Internet et, plus largement, le cyberespace offrent de nombreuses possibilités ainsi que des vulnérabilités et des risques nouveaux et en constante évolution. C'est pourquoi ce guide contient des conseils utiles sur la sécurité des réseaux et la cybersécurité.



5 PROTECTION DE LA VIE PRIVÉE

5.1 Principaux concepts

Le RGPD établit les règles relatives au traitement des données à caractère personnel et les règles relatives à la libre circulation de ces données (art. 1). L'objectif est de protéger les droits et libertés fondamentaux des personnes physiques et en particulier leur droit à la protection des données à caractère personnel.

Ce processus est généralement associé au terme de protection de la vie privée.

Chaque entreprise doit traiter les données personnelles pour leur bon fonctionnement. Par conséquent, toute PME européenne doit aborder correctement la question de la conformité au RGPD. Ce document fournit des conseils de base sur la conformité au RGPD. Ils sont basés sur la norme ISO/CEI 27701, une norme qui étend les normes ISO/CEI 27001 et 27002 en fournissant des exigences et des lignes directrices pour le management des informations personnelles. Cela rend l'approche saine et, au besoin, jette les bases de la conformité dans d'autres juridictions.

Toutefois, il convient de considérer que ce document ne vise pas à être exhaustif, mais à aider les PME à adopter les contrôles les plus importants. Pour cette raison, compte tenu également de la sensibilité du sujet et des amendes élevées en cas de traitement non conforme, il est toujours nécessaire de vérifier le texte du RGPD. Il est fortement recommandé aux PME de lire et d'appliquer la norme ISO/CEI 27701, pour laquelle ce guide peut être une introduction utile. C'est particulièrement le cas lorsque le traitement des données personnelles fait partie du cœur de métier de la PME.

Lorsque la PME met en œuvre un type de traitement susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées, elle évalue l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel (voir art. 35 du RGPD pour plus de détails). Un outil supplémentaire est une certification prévue aux art. 42 et 43 du RGPD et décrite à la section 5.2. Une fois établi, il constituera un outil utile pour réduire le risque de non-conformité.

5.2 Attestations liées à la protection des données personnelles

La norme ISO/CEI 27001 soutient une certification par un tiers en tant que système de management de la sécurité de l'information ; par conséquent, un organisme de certification qui opère sous accréditation et certifie la conformité à cette norme doit être accrédité conformément à la norme ISO 17021-1:2015, une norme qui précise « les principes et les exigences pour la compétence, la cohérence et l'impartialité des organismes d'audit et de certification de tous les types de systèmes de management ».[6]

L'Art. 42 du règlement (UE) 2016/679 encourage la mise en place de mécanismes de certification de la protection des données afin de démontrer la conformité au RGPD des traitements effectués par les responsables du traitement et les sous-traitants.

[6] Tous les organismes de certification DOIVENT être accrédités, sinon le certificat SMSI/RGPD n'est pas valide et reconnu. La certification démontre la conformité (pour une période de 3 ans). La certification n'est pas obligatoire mais volontaire. La plupart des organisations (et des PME) choisissent une mise en œuvre vérifiée par un tiers de confiance.

En outre, l'Art. 43 établit les caractéristiques des organismes de certification qui certifieront la conformité du traitement des données à caractère personnel avec le RGPD ; ces organismes doivent être accrédités soit par l'autorité de surveillance, soit par l'organisme national d'accréditation conformément à la norme ISO/CEI 17065:2012, qui définit les exigences en matière de compétence, de fonctionnement cohérent et d'impartialité des organismes de certification pour les produits, processus et services.

ISO/CEI 27701 est une extension de la norme ISO/CEI 27 001, il est donc nécessaire que l'organisme de certification soit accrédité selon la norme ISO 17021-1:2015, comme pour la norme ISO/CEI 27 001. Par conséquent, il n'est pas possible d'utiliser la norme ISO/CEI 27701 comme base pour une certification conforme à l'article 42, car l'article 43 exige que l'organisme de certification soit accrédité par la norme ISO/CEI 17065:2012.

Par conséquent, bien que le RGPD (Règlement [UE] 2016/679) exige une certification de type « produit » pour démontrer la conformité au RGPD, la norme ISO/CEI 27 701 est certifiable en tant qu'extension de la norme ISO/CEI 27 001 et exige une certification de type « système de management ».

Afin de démêler ce paquet qui a été créé entre ISO/CEI 17 021 et ISO/CEI 17065, il est souhaitable que l'European Data Protection Board (EDPB) soit en mesure de déclarer valide ou non la certification selon l'extension ISO/CEI 27701:2019. C'est la seule façon de maintenir l'un des principes clés sur lesquels repose le RGPD : des règles égales pour le traitement des données dans tous les États membres de l'UE.

Les organisations qui ont déjà mis en œuvre un SMSI (Système de management de la sécurité de l'information) selon ISO/CEI 27 001 peuvent l'étendre à la gestion de la vie privée, y compris le traitement des données personnelles, en utilisant ISO/CEI 27701. Les organisations qui ne disposent pas d'un SMSI peuvent également mettre en œuvre les normes ISO/CEI 27001 et 27701 en un seul projet, car la norme ISO/CEI 27701 étend simplement les exigences fournies par la norme 27001 et son code de conduite (ISO/CEI 27002). Il n'est donc pas nécessaire d'effectuer deux certifications distinctes.

Une certification basée sur ISO/CEI 27701 est un outil internationalement reconnu qui peut aider à démontrer la conformité à la législation sur la protection des données, même si elle n'est pas strictement conforme à l'art GDPR. 42 concernant la certification.

Tout ceci est en attente de clarification du potentiel de la norme ISO/CEI 27701comme moyen de démontrer la conformité au RGPD du traitement des données à caractère personnel effectué en tant que responsable de traitement ou sous-traitant.

Dans tous les cas, un système de management des informations à caractère personnel (PIMS) conforme à la norme ISO/CEI 27701 est utile pour toute organisation ayant des obligations en matière de protection des données. Il présente un intérêt particulier pour les organisations qui opèrent à l'échelle internationale, travaillent avec des clients dans d'autres juridictions ou opèrent dans des chaînes d'approvisionnement internationales. Ces organisations sont souvent tenues de se conformer à divers règlements et lois sur la protection de la vie privée, et cette nouvelle norme peut simplifier la conformité.

En mettant en œuvre un PIMS comme extension d'un SMSI conforme à la norme ISO/CEI 27001, une organisation peut collecter et traiter des données, y compris des données personnelles, de manière systématique. Ils peuvent également gérer les risques associés à la confidentialité, à l'intégrité et à la disponibilité de l'information, et réagir aux menaces et aux risques changeants qui pèsent sur les données et la vie privée.

Un PIMS permet également aux organisations de réduire les coûts associés à la protection de la vie privée et à la sécurité de l'information en s'adaptant constamment aux changements dans l'environnement et au sein de l'organisation, augmentant ainsi la résilience aux cyberattaques.

Un PIMS présente plusieurs avantages :

- Renforcer la confiance dans la capacité de votre entreprise à gérer les données personnelles, tant pour les clients que pour les employés.
- Aider à démontrer la conformité au RGPD et aux autres réglementations applicables en matière de vie privée.
- Clarifier les rôles et responsabilités au sein de votre organisation.
- Améliorer les compétences et les processus internes pour éviter les failles.
- Assurer la transparence des contrôles établis de gestion de la vie privée.
- Faciliter les ententes avec les partenaires commerciaux lorsque le traitement des données personnelles (PII) est mutuellement pertinent.
- Intégration facile avec la norme principale de sécurité de l'information ISO/CEI 27001.

ISO/CEI 27701 fournit un ensemble d'annexes qui aident à l'élaboration de contrôles appropriés, tant pour la mise en œuvre des mesures de sécurité et de conformité nécessaires que pour l'élaboration d'évaluations des risques.

5.3 Contrôles concernant la protection de la vie privée

ISO/CEI 27701 est un outil conçu pour traiter correctement les questions de sécurité et de gestion des risques liés au traitement des données personnelles. Ce faisant, il « s'appuie » sur l'ISO/CEI 27001, créant de la valeur et les conditions d'une intégration rapide. Il en va de même pour les contrôles concernant la protection de la vie privée de la norme ISO/CEI 27701 inclus dans la section 7, qui décrit les contrôles de sécurité des informations les plus importants basés sur les normes ISO/CEI 27001 et ISO/CEI 27701.

Pour chaque contrôle, un sous-alinéa spécifique (Extension à la vie privée) est ajouté lorsqu'un contrôle

général défini dans la norme ISO/CEI 27001 est spécialisé par la norme ISO/CEI 27701. Des contrôles spécifiques et supplémentaires concernant la protection de la vie privée sont décrits à la fin de la section 7 (contrôles 14 à 16).

6 GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION

6.1 Qu'est-ce que la gouvernance de la sécurité de l'information?

La gouvernance de la sécurité de l'information vise l'organisation et l'utilisation adéquate des ressources pour assurer la mise en œuvre efficace de la sécurité de l'information et fournit l'assurance que :

- les directives concernant la sécurité de l'information seront suivies ; et
- l'organe directeur recevra des rapports fiables et pertinents sur les activités liées à la sécurité de l'information.

La mise en œuvre de contrôles de sécurité sans stratégie et objectifs clairs peut les rendre inefficaces et même préjudiciables à l'organisation. Pour cette raison, la gouvernance d'entreprise est essentielle. La gouvernance des TIC dirige la mise en œuvre des technologies de l'information et des communications et la gouvernance de la sécurité de l'information oriente la gestion de l'information. Ce sont deux composantes de la gouvernance d'entreprise.
La gouvernance d'entreprise de l'information et de la technologie (EGIT) est complexe et comporte de multiples facettes. Par conséquent, les membres des conseils d'administration et de la haute direction doivent généralement adapter leurs mesures EGIT et les mettre en œuvre en fonction de leur contexte et de leurs besoins particuliers.

Fondamentalement, l'EGIT s'intéresse à la prestation de valeur découlant de la transformation numérique et à l'atténuation des risques opérationnels qui en découlent. Plus précisément, trois principaux résultats peuvent être attendus après l'adoption réussie de l'EGIT :

- réalisation des avantages et bénéfices
- optimisation des risques
- optimisation des ressources.

6.2 ISO/CEI 27014

En ce qui concerne la gouvernance de la sécurité de l'information, la norme ISO/CEI 27014 établit la stratégie à suivre. Elle définit 6 objectifs :

1. assurer une approche de sécurité de l'information à l'échelle de l'organisation qui est alignée sur les objectifs d'affaires ;
2. veiller à ce que les décisions soient prises selon une approche fondée sur les risques ;
3. veiller à ce que l'acquisition de produits et de services respecte un processus et une direction définis [établir la direction de l'acquisition] ;
4. s'assurer que la sécurité de l'information est conforme aux exigences internes et externes ;
5. favoriser une culture de sécurité positive ;
6. s'assurer que les performances de sécurité respectent les exigences actuelles et futures de l'organisation.

Ces objectifs peuvent être atteints si une stratégie de gouvernance de la sécurité est établie en fonction des quatre processus suivants :

1. évaluer ;
2. diriger ;
3. surveiller ;
4. communiquer.

L'ISO/CEI 27 014 établit une distinction entre l'organe directeur qui évalue, dirige et surveille ; et l'organe de direction, en charge de la mise en œuvre du SMSI reposant sur l'ISO/CEI 27001.

Comme d'habitude avec les normes, ISO/CEI 27014 nous dit quoi faire, mais pas comment le faire ; et des connaissances spécialisées sont nécessaires pour apporter la stratégie définie par l'organe directeur aux processus et procédures concrets et mesurables. Cette connaissance peut être fournie par le COBIT.

6.3 COBIT

Qu'est-ce que le COBIT ?

COBIT (Control Objectives for Information and related Technology [I&T]) est un cadre de gouvernance et de gestion de l'information et de la technologie d'entreprise, y compris sur les questions de sécurité, destiné à l'ensemble de l'entreprise. L'I&T d'entreprise désigne toutes les technologies de traitement de l'information que l'entreprise met en place pour atteindre ses objectifs, peu importe où cela se produit dans l'entreprise. En d'autres termes, l'I&T d'entreprise n'est pas limité au département informatique d'une organisation, mais l'inclut certainement.

Le cadre COBIT établit une distinction claire entre gouvernance et management. Ces deux disciplines englobent des activités différentes, nécessitent des structures organisationnelles différentes et servent à des fins différentes.

La gouvernance garantit que :

- les besoins, les conditions et les options des parties prenantes sont évalués pour déterminer des objectifs d'entreprise équilibrés et convenus ;
- la guidance est établie par la priorisation et la prise de décisions ;
- la performance et la conformité sont surveillées par rapport à la guidance et aux objectifs convenus.

Le management planifie, élabore, exécute et surveille les activités, conformément à la guidance établie par l'organisme de gouvernance, pour atteindre les objectifs de l'entreprise.

Structure du COBIT :

Pour que l'information et la technologie contribuent aux buts de l'entreprise, un certain nombre d'objectifs de gouvernance et de management devraient être atteints. Les objectifs de gouvernance et de management du COBIT sont regroupés en cinq domaines (1 à la section A et 4 à la section B) :

- A. Les objectifs de gouvernance sont regroupés dans le domaine Évaluer, Diriger et Surveiller (EDM). Dans ce domaine, l'organe directeur évalue les options stratégiques, dirige le management sur les options stratégiques choisies et surveille la réalisation de la stratégie.
- B. Les objectifs de management sont regroupés dans les quatre autres domaines :
  - Aligner, Planifier et Organiser (**APO)** concerne l'organisation globale, la stratégie et les activités de soutien pour l'I&T ;
  - Construire, acquérir et mettre en œuvre (**BAI)** traite la définition, l'acquisition et la mise en œuvre des solutions I&T et leur intégration dans les processus opérationnels ;
  - La **prestation, le service et le soutien** (SSM) porte sur la prestation et le soutien opérationnels des services d'I et T, y compris la sécurité ;
  - La surveillance, l'évaluation et l'évaluation (**MEA)** porte sur la surveillance de la performance et la conformité de l'I&T avec les cibles de performance internes, les objectifs de contrôle interne et les exigences externes.

Pourquoi COBIT ?

L'application de la méthodologie COBIT à la sécurité de l'information offre plusieurs avantages, notamment :

- une réduction de la complexité et une rentabilité accrue grâce à une intégration et à une harmonisation améliorées et plus faciles des normes de sécurité de l'information, des bonnes pratiques et/ou des lignes directrices propres au secteur ;
- une plus grande satisfaction des intervenants grâce à une meilleure compréhension de la sécurité de l'information et de ses résultats ;
- une meilleure intégration de la sécurité de l'information à l'échelle de l'organisation ;
- des décisions plus éclairées en matière de risque et une meilleure sensibilisation aux risques ;

- une amélioration de la prévention, de la détection et de la récupération (recovery) ;
- une réduction — en termes d'impact et de probabilité — des incidents de sécurité de l'information ;
- un meilleur soutien à l'innovation et à la compétitivité ;
- une meilleure gestion et optimisation des coûts liés à la sécurité de l'information ;
- une meilleure compréhension de la sécurité de l'information par les parties prenantes.

7 CONTRÔLES DE LA SÉCURITÉ DE L'INFORMATION ET DE LA PROTECTION DE LA VIE PRIVÉE

7.1 Introduction

La norme ISO/CEI 27002 comprend 114 contrôles de sécurité ! Reconnaissant la complexité et les coûts de mise en œuvre pour les PME, cette section introduit et recommande la mise en œuvre de 16 contrôles[7] pour assurer une protection minimale et efficace des données des entreprises. Ils concernent différents niveaux de protection et sont classés comme suit :

Catégorie	Contrôle
Personnel	**Contrôle #13** : Sensibilisation à la sécurité de l'information
Organisationnel	**Contrôle #1 :** Gestion des actifs (incl. Procédure de classification) **Contrôle # 2 :** Politiques, normes et lignes directrices **Contrôle # 3 :** Gestion des incidents **Contrôle #14 :** Aspects de sécurité de l'information en relation avec les fournisseurs **Contrôle #15 :** Organisation de la sécurité de l'information **Contrôle #16 :** Contrôles de confidentialité supplémentaires
Partiellement organisationnel/technique	**Contrôle #4 :** Gestion du contrôle d'accès

[7] Certains des 16 contrôles de la section 7.2 comprennent plusieurs contrôles inter-reliés de la norme ISO/CEI 27002. Le numéro des contrôles fait référence aux contrôles présentés à la section 7.2.

Technique (lié aux TIC)	**Contrôle # 5 :** Sécurité du réseau et échange de données **Contrôle # 6 :** Gestion des vulnérabilités **Contrôle #7 :** Combattre les logiciels malveillants **Contrôle #8 :** Gestion des backups **Contrôle #9 :** Gestion des mesures de protection **Contrôle #10 :** Préparation des TIC à la continuité des activités **Contrôle #11 :** Télétravail **Contrôle #12 :** Surveillance des cybermenaces

La catégorie personnelle vise à sensibiliser le personnel des PME à la sécurité de l'information. Le contrôle vise à établir des lignes directrices à l'intention du personnel et des utilisateurs des PME, afin qu'ils respectent les objectifs de sécurité de l'information par la sensibilisation, la formation et l'éducation.

La catégorie organisationnelle cible le côté management de la sécurité de l'information à l'aide de la matrice RACI. En organisant sa sécurité de l'information, une PME doit définir et attribuer les rôles de sécurité essentiels au personnel responsable avec des mécanismes définis pour rendre compte à la direction. En outre, une PME devrait :

- gérer et protéger ses actifs numériques ;
- répondre adéquatement aux incidents compromettant ses données ;
- élaborer des politiques et des lignes directrices pour assurer et maintenir la conformité en matière de management de l'information ;
- partager des informations pertinentes et fiables avec leurs fournisseurs et assurer une gestion et une protection adéquates des données partagées avec les fournisseurs disposant de mécanismes d'intervention suffisants en cas d'incidents ;
- Le contrôle no 16 décrit les contrôles supplémentaires définis dans la norme ISO/CEI 27701 qui portent exclusivement sur la protection de la vie privée qui a été jugée importante pour les PME.

L'accès à l'information implique des compétences à la fois managériales et techniques pour maintenir un accès continu aux données par des personnes autorisées. La gestion du contrôle d'accès traite de ces questions.

Enfin, **la catégorie technique (liée aux TIC)** couvre la plupart des travaux techniques liés à la protection du réseau de l'entreprise. Ces contrôles portent sur les questions suivantes :

- faciliter les échanges de données et mettre en place des procédures appropriées pour la sauvegarde des données et le travail à distance ;
- traiter et gérer les vulnérabilités, les cybermenaces et les logiciels malveillants ;
- assurer des mesures de protection adéquates et maintenir la continuité des activités après une cyberattaque.

Comme expliqué dans la section 5, l'ISO/CEI 27701 étend les exigences fournies par l'ISO/CEI 27001 et étend les contrôles spécifiés dans l'ISO/CEI 27 002. Cette section utilise la même approche : un paragraphe pour

chaque contrôle de sécurité de l'information considéré comme pertinent pour les PME ; et, lorsqu'un contrôle de sécurité de l'information a dans la norme ISO/CEI 27701 une exigence supplémentaire en matière de vie privée, un sous-alinéa nommé « Extension à la vie privée » a été ajouté à ce contrôle.

Il est important de noter que les 16 contrôles présentés ci-dessous sont les recommandations minimales que les PME doivent mettre en œuvre pour se conformer aux exigences du RGPD.

7.2 Contrôle

Tous les contrôles décrits ci-dessous suivent la même structure. Une fois qu'un contrôle est énoncé, il est suivi d'une « guidance » qui montre ce que les PME devraient faire pour mettre en œuvre le contrôle et atteindre son objectif. Cette guidance fournit la **référence « minimale » à mettre en œuvre.** Comme l'illustre la section 4, ces contrôles ne sont PAS assujettis à la gestion des risques.
La structure de chaque contrôle est la suivante :

- **Contrôle :** énoncé clair d'une action à entreprendre et à accomplir.
- **Objectif :** donne, autant que possible, l'objectif que le contrôle entend atteindre, de manière SMART[8].
- **Portée :** l'environnement que le contrôle vise à couvrir.
- **Situation :** une vision pragmatique de la situation actuelle du contrôle au sein des PME. Certaines PME sont, bien sûr, beaucoup plus conformes et habituées aux bonnes pratiques.
- **Guidance :** liste des mesures à prendre pour réaliser le contrôle, accompagnée, le cas échéant, d'une procédure pratique dans une annexe.
- **Protection de la vie privée :** quelques considérations reliant les lignes directrices à la protection des données personnelles.

[8] SMART signifie : spécifique et simple, mesurable (donc concret), réalisable/acceptable/ambitieux (suffisamment pour motiver les gens à agir), réaliste et limité dans le temps. En règle générale, le T doit être considéré comme « CONTINU » puisque les contrôles proposés sont considérés comme une base minimale sans laquelle aucune gestion réelle de la sécurité de l'information n'est possible.

8 CONTRÔLE #1 : GESTION DES ACTIFS

Contrôle

La gestion des actifs devrait être en place pour permettre le traitement approprié de l'information et des biens connexes et décider du niveau de protection approprié.

Objectif

Les PME veilleront à ce que leurs investissements (y compris en matière de sécurité et de protection) soient justifiés.

Portée

Ce contrôle concerne l'information, les processus, les supports contenant l'information, l'équipement TIC stockant, manipulant et transmettant l'information, et les espaces physiques où se trouvent tous les précédents. Ce contrôle est un complexe de sept contrôles coordonnés qui sont tous nécessaires pour atteindre l'objectif proposé.

Situation

Les actifs, le mobilier et les consommables TIC sont gérés à minima simplement, alors que l'information ne l'est pas du tout. La gestion des actifs comprend les éléments suivants :

- **L'acquisition d'actifs** permet aux PME de connaître et d'enregistrer le fournisseur, et les actifs sont généralement achetés auprès de fournisseurs de confiance. Ce n'est toutefois guère le cas avec l'information : la source ne semble pas importante et n'est pas enregistrée. Quand il y a un problème avec l'information, il n'y a aucun moyen de se plaindre. Si l'information est essentielle à la PME, il n'y a rien à faire.
- **Identification et valorisation des actifs :** Si l'identification et la valorisation sont fréquentes et indispensables dans le cas des actifs physiques, elles le sont rarement dans le cas des informations. Il n'y a pas d'inventaire de l'information ni des médias sur lesquels l'information est stockée, et l'information ne reçoit pas

de valeur. Cette dernière activité est appelée « Classification de l'information ». La valeur de l'actif est un facteur crucial pour déterminer les conséquences d'un risque qui devient réalité. La valeur facilite également la décision sur la force et la résistance de la protection (d'où son prix). La détermination de la valeur de l'information permet aux PME d'évaluer le risque d'atteinte à la confidentialité, à l'intégrité et à la disponibilité, et de déterminer ce que vous pourriez faire (valeur par rapport au coût) pour contrer le risque.

- **Stockage des actifs :** Les actifs qui ne sont pas utilisés directement sont stockés et l'évolution du stock est enregistrée. L'équipement TIC est stocké selon les spécifications du fournisseur et l'argent est dans un coffre-fort.

L'information est stockée dans des dossiers, des classeurs ou des registres, et dans la mémoire des ordinateurs. Il n'y a toutefois aucune idée claire de l'emplacement de l'information et de son statut. Cela signifie qu'il est possible que tous les utilisateurs n'utilisent pas la même version de l'information. Il n'y a généralement pas de sécurité pour les informations critiques.

- **Utilisation des actifs :** Les actifs sont utilisés selon les recommandations du fournisseur, et des politiques et des règles existent. Les actifs TIC portent une étiquette indiquant le propriétaire et son code d'inventaire.
  L'information est utilisée au moyen de processus opérationnels qui contrôlent le flux et les opérations qui en découlent. Les processus d'information ne sont pas toujours décrits formellement (même dans les grandes entreprises), ce qui pose des problèmes lorsque le processus est automatisé dans un programme informatique.

- **Entretien des actifs :** Les actifs sont entretenus conformément aux recommandations du fournisseur. Il y a cependant peu d'entretien sur l'information. Plusieurs versions peuvent exister, et peu de contrôle est fait.

- **L'échange d'actifs** au sein de l'entreprise et avec des tiers est enregistré. Le transport se fait par des canaux reconnus et l'emballage garantit qu'il n'y a aucun dommage pendant le transport.
  Les échanges d'information se produisent souvent sans protection adéquate, et il y a généralement un faible contrôle sur qui peut y mettre la main.

- **Évacuation des biens :** Lorsque des biens sont endommagés, périmés ou inutilisables, ils sont jetés, peut-être par des circuits écologiques. Malheureusement, l'information est généralement simplement « supprimée », et les supports d'information sont jetés sans attention à ce qu'ils contenaient et s'ils ont été correctement effacés.

Guidance

L'ISO/CEI 27002 recommande de gérer l'information comme un actif essentiel.

- **L'information devrait provenir de sources fiables.** Les informations provenant d'Internet devraient être revérifiées.

Par exemple, les données à caractère personnel (DCP) — Données personnelles dans le RGPD — fournies par les employés, les clients et les fournisseurs doivent être vérifiées et les données financières et comptables doivent être continuellement contrôlées et surveillées. Il devrait en être de même pour l'information qui a de la valeur pour la PME.

- **Les informations devraient être inventoriées et classifiées** en fonction des trois critères de sécurité — confidentialité, intégrité, disponibilité — selon leur importance pour atteindre les objectifs opérationnels. L'Annexe A propose une technique simple pour classifier l'information et les biens matériels qui

contiennent et manipulent l'information.

Il n'est pas nécessaire de procéder à la classification et à l'inventaire de l'information pour chaque élément d'information, sauf pour ceux qui ont la plus grande valeur. Il est cependant plus pratique de donner la même classification à chaque catégorie d'information (par exemple, DCP pour se conformer au RGPD). L'inventaire des informations devrait indiquer la source et la date d'acquisition, car, dans bien des cas, l'information devient rapidement périmée. **Note :** Dorénavant, les « **informations protégées** » désignent les informations qui obtiennent le niveau 3 ou plus avec la technique de l'Annexe A).

- **Les informations protégées devraient être étiquetées**. Les fichiers de données informatiques peuvent recevoir leur étiquette dans les champs disponibles des « Propriétés du fichier ». L'indication de la confidentialité, de l'intégrité et/ou de la disponibilité est recommandée. L'étiquetage dans le pied de page ou l'en-tête du document est également une bonne solution.
- Les supports de données devraient recevoir une étiquette selon le niveau de confidentialité (par exemple en utilisant un code couleur) pour indiquer au personnel comment ils devraient les manipuler.
- Les informations devraient être stockées selon leur étiquette de classification, quel que soit leur support ou leur format, avec des règles spécifiques supplémentaires pour les informations protégées.
    - Des mesures de protection et des sauvegardes pour l'information et les applications devraient exister, proportionnelles à la valeur de l'information (tout comme les valeurs financières), p. ex., nombre, fréquence et emplacement ;
    - Des mesures devraient être en place pour assurer la préservation de l'intégrité de l'information, quelle que soit la durée du stockage ; les informations protégées devraient faire l'objet de tests réguliers pour vérifier qu'elles sont lisibles et utilisables lorsqu'elles sont récupérées ;
    - Des contrôles d'accès devraient être en place pour s'assurer que seules les personnes et les applications autorisées y ont accès dans des conditions précises (voir le contrôle #4).
- L'information sous le niveau « protégé » doit être manipulée et utilisée avec un soin standard. Les informations protégées ne doivent être utilisées que par le personnel autorisé et selon les règles spécifiques énoncées dans les politiques (voir Contrôle #2), car toute mauvaise utilisation, même accidentelle, peut mettre l'entreprise en danger.
- Les informations protégées devraient suivre un processus de tenue à jour officiel pour s'assurer qu'ils demeurent pertinents, exacts et disponibles.
- L'échange et la communication d'information sont essentiels à la réalisation des objectifs d'entreprise. Des règles devraient toutefois être en place et documentées pour garantir que les informations protégées ne sont échangées qu'avec les parties prenantes internes et externes autorisées et dans un conteneur adéquat (p. ex., scellé avec inventaire du contenu, chiffré, VPN, etc.). La communication d'informations protégées à des parties externes :
    - devrait être interdite pendant les discussions informelles et dans les lieux publics ;
    - lors de discussions formelles, de réunions et de conférences, cela devrait se faire selon des règles spécifiques et avec l'autorisation formelle de la direction de l'entreprise.
- Dans le cas où l'information devient inutile ou n'est plus pertinente pour l'entreprise, cela ne signifie pas qu'elle a perdu sa valeur pour d'autres parties (non autorisées) :

- en fait, ces tiers non autorisés pourraient découvrir quelque chose qu'ils pourraient utiliser à leur propre avantage et peut-être contre vous ;
- de plus, les mémoires numériques mises au rebut (clés USB, disques durs, etc.) pourraient contenir des logiciels et des applications pour lesquels vous avez payé la licence, et une utilisation illégale ultérieure par des tiers peut vous causer des problèmes juridiques ;
- Les informations doivent être éliminées avec soin et la règle habituelle est qu'elles doivent être effacées ou détruites. Les informations protégées doivent être déchiquetées (papier, cartes bancaires, CD/DVD), dûment effacées ou chiffrées (données numériques).

Extension à la vie privée

La protection des données personnelles est une catégorie spéciale d'informations qui exige un processus de classification différent, qui est fourni par une évaluation des impacts sur la vie privée (PIA) qui mesure l'incidence des atteintes à la sécurité sur la personne concernée.

10 CONTRÔLE # 2 : POLITIQUES, NORMES ET LIGNES DIRECTRICES

Contrôle

Des informations documentées devraient exister pour déclarer et publier vers toutes les parties prenantes les objectifs, les directives, les exigences et les lignes directrices en matière de sécurité de l'information.

Objectif

Les PME veillent à ce que le personnel et toutes les personnes impliquées dans le traitement des informations de l'entreprise connaissent et respectent les règles. Ce faisant, la PME devrait être et demeurer

conforme aux exigences externes et juridiques liées à l'information.

Portée

Ce contrôle concerne tous les objectifs, règles et recommandations auxquels les parties internes et externes concernées doivent se conformer.

Situation

Les PME ne documentent guère leurs objectifs, règles et attentes en matière de management et de sécurité de l'information, alors qu'elles le font pour les ressources humaines et les finances. Cependant, selon le contrôle 9.1.1 de la norme ISO/CEI 27 002 — et le Contrôle #1 ci-devant, l'information a une valeur très importante qui doit être protégée.

Guidance

Les objectifs, règles et directives en matière de sécurité de l'information devraient être documentés et communiqués à tout le personnel pour s'assurer qu'ils sont fixés, connus et appliqués.
Deux politiques importantes devraient être disponibles :

- la politique globale de sécurité de l'information qui fixe les objectifs à atteindre sur une base continue et qui contient ceux qui sont censés être conformes au RGPD (Politique de protection de la vie privée) ;
- la politique de confidentialité qui énonce, pour les personnes dont vous recueillez et manipulez les données personnelles (personnel, clients, fournisseurs, partenaires), les informations dont vous avez besoin, avec qui vous les partagez et pour quelle raison, la durée de leur conservation, comment elles peuvent utiliser leurs droits et comment déposer une plainte lorsqu'ils sentent que les choses vont mal.

Des règles spécifiques concernant le stockage, la manipulation, le contrôle d'accès, la destruction, les backups et la communication avec des parties externes pourraient également être documentées :

- une **norme** est une règle qui doit être appliquée en toutes circonstances et qui peut être invoquée pour des sanctions en cas de non-application ;
- une **directive** est une recommandation concernant la « meilleure façon » de traiter l'information et sa sécurité.

Il est essentiel que les « politiques » soient approuvées par le cadre supérieur et qu'elles soient régulièrement examinées et mises à jour pour tenir compte des changements dans les conditions et les circonstances opérationnelles. La recommandation est un examen annuel. Les « politiques » devraient être pertinentes et axées sur les personnes qu'elles visent. La taille et la formulation dépendent de votre situation et de vos besoins spécifiques. La documentation est la base clé pour informer, former et éduquer les gens.

Extension à la vie privée

Une politique spécifique concernant la protection de la vie privée devrait être préparée et régulièrement révisée.

11 CONTRÔLE #3 : GESTION DES INCIDENTS

Contrôle

Les incidents de sécurité de l'information devraient être gérés.

Objectif

Les PME devraient être prêtes à réagir adéquatement aux incidents liés à la sécurité de l'information. Elles s'assureront ainsi une résolution rapide et cohérente de toutes les perturbations opérationnelles, financières, juridiques et commerciales et de maintenir les dommages dans des limites prédéfinies.

Portée

Ce contrôle concerne tous les incidents causés par des atteintes à la confidentialité, à l'intégrité et à la disponibilité de l'information. Ce contrôle concerne évidemment aussi les atteintes à la vie privée.

Situation

La gestion des risques, peu appliquée dans les PME, n'est pas toujours parfaite, et le risque zéro n'existe pas. Par exemple, un incendie peut se produire même si toutes les mesures préventives sont prises. Les humains peuvent faire des erreurs et des défaillances techniques peuvent survenir.

Comme l'information est généralement mal gérée et mal protégée, de nombreux événements et incidents se produisent, sans être remarqués et traités comme il se doit. Si l'impact direct n'est pas important, les

conséquences commerciales se produisent plus tard et peuvent être énormes sans aucun lien possible avec l'incident.

Guidance

Quoi que vous fassiez, les mesures que vous prenez et les contrôles que vous mettez en œuvre et gérez pour contrer les risques, les événements se produiront et perturberont vos activités. S'ils ont une incidence sur vos objectifs, ils deviendront un incident commercial. S'ils ont une incidence sur les objectifs de sécurité de l'information, ils deviendront des incidents de sécurité de l'information. La seule norme ISO/IEC décrivant les concepts, les principes et le processus de gestion des incidents est la norme ISO/CEI 27035-1. Les recommandations qui suivent donnent un aperçu de ce qui doit être fait pour être en mesure de réagir de façon satisfaisante à ces incidents.
Il est crucial de préparer la réponse aux incidents avec des procédures prédéfinies et testées, ainsi que par la formation, le personnel pour signaler les événements et les situations anormales et les équipes spécialisées qui seront dédiées à la réponse.
La gestion cohérente des incidents comporte cinq phases :

1. **Planifier et préparer**

Dans cette phase, l'entreprise décide de traiter les incidents pour éviter qu'ils ne deviennent ingérables. Pour ce faire, il faut :

- préparer une politique pour organiser et gérer les incidents ;
- désigner une personne de la haute direction responsable de la gestion des incidents ;
- dresser la liste des incidents que vous souhaitez gérer ;
- documenter (avec des experts internes et externes au besoin) la ou les procédures que vous avez l'intention d'adopter lorsque l'incident se produit ;
- décider et installer la personne responsable de la gestion de l'incident et de la coordination des actions (gestionnaire de l'incident) ;
- déterminer les critères et la procédure de déclaration d'un incident ;
- décider et installer l'équipe qui répondra à l'incident conformément à la procédure ;
- déterminer et installer les moyens nécessaires pour que le gestionnaire de l'incident soit informé, ainsi que le type d'information à transmettre. Ils peuvent être automatisés ou activés ;
- préparer et mettre en œuvre un plan de sensibilisation et de formation pour s'assurer que tous les acteurs savent quoi faire.

2. **Détecter**

Assurez-vous que tout le personnel a la capacité de signaler l'événement au gestionnaire de l'incident sans risquer de pénalité (nous le faisons tous en cas d'incendie ou de blessures). Cela devrait se faire sans retard injustifié, car un retard dans l'intervention pourrait entraîner une catastrophe.

3. **Évaluer et décider**

Le gestionnaire de l'incident suit la procédure d'évaluation de l'événement et le déclare comme incident.

- S'il ne s'agit pas d'un incident, le gestionnaire de l'incident informe la personne responsable du processus, de l'actif ou des services de TIC de la situation, ce qui lui permet de chercher une correction.
- S'il s'agit d'un incident, le gestionnaire de l'incident active l'équipe d'intervention qui a les compétences et la capacité d'agir (interne ou externe).

4. Répondre

Le gestionnaire de l'incident demeure responsable de la coordination des actions jusqu'à ce que l'incident soit déclaré clos. Il consigne les mesures prises au fil de l'incident. L'équipe d'intervention communique régulièrement avec le gestionnaire de l'incident pour le tenir au courant de l'évolution :

- Si la situation s'aggrave ou a besoin de ressources supplémentaires, le gestionnaire de l'incident les appelle, après autorisation de la haute direction si nécessaire.
- Si la situation semble devenir incontrôlable, le gestionnaire de l'incident appelle la haute direction, et le plan de continuité d'activité est activé (en partie ou complètement).

Le responsable de l'incident déclare l'incident clos après discussion et avec l'approbation de l'équipe concernée.

Une fois l'incident clos, le gestionnaire de l'incident remplit le rapport d'incident à l'aide du modèle prédéfini et le transmet à la haute direction.

Lorsqu'il faut prendre des mesures supplémentaires après l'incident (p. ex., criminalistique), le responsable de l'incident tient les équipes au courant de l'évolution.

5. Tirer des leçons

Chaque événement ou incident ainsi que la façon dont l'intervention s'est déroulée fournissent des renseignements essentiels sur la capacité de les prévenir et de les gérer à l'avenir. C'est la source des leçons apprises. Une équipe (peut-être celle qui a préparé le plan de gestion ou de réponse) se réunira et verra ce qui peut être amélioré :

- une meilleure prévention de l'événement (amélioration des contrôles ou des procédures opérationnelles) ;
- une meilleure capacité de réponse (ressources, compétences, équipement de soutien) ;
- amélioration des rapports et de la communication.

6. Renseignements supplémentaires

Dans certains cas, le RGPD exige que la personne ou les personnes concernées ou l'Autorité de protection des données — la « partie externe » — soient informées. Les règles opérationnelles devraient également faire en sorte que le « propriétaire d'une information (à laquelle l'entreprise a accès) » soit informé si

quelque chose lui arrive. De même, lorsqu'une personne peut être affectée par une erreur, un bug ou un incident, ils doivent être informés pour être en mesure de réagir adéquatement. Dans certains cas, la « partie externe » peut également aider l'entreprise à résoudre le problème.
Pour ce faire, un plan de communication devrait être documenté indiquant qui est autorisé à communiquer à l'extérieur de l'entreprise, et comment. Une mauvaise communication peut avoir de graves répercussions sur la réputation de l'entreprise.

Extension à la vie privée

Les incidents liés aux données personnelles suivent le processus générique pour un incident de sécurité de l'information. Le RGPD exige que, selon l'impact sur la personne concernée, cette dernière et l'autorité nationale de protection des données soient informées, dans un délai de 72 heures.

12 CONTRÔLE #4 : GESTION DU CONTRÔLE D'ACCÈS

Contrôle

Le contrôle de l'accès devrait être entièrement et continuellement géré dans toutes ses composantes et fondé sur le rôle pour atteindre les objectifs opérationnels.

Objectif

Les PME maîtriseront l'accès à l'information quelles qu'elles soient, où qu'elles soient et en tout temps.

Portée

Ce contrôle est composé de plusieurs contrôles interdépendants qui doivent être définis et mis en œuvre simultanément pour atteindre les objectifs. Ce contrôle concerne l'accès à l'information (numérique ou sur support physique) et les installations opérationnelles telles que les bureaux et les équipements TIC.
Situation

Trop souvent, le contrôle d'accès réside sur les PC et consiste en un identifiant (ID) et un mot de passe (généralement faible et identique pour tous les usages). Une fois que l'utilisateur est « à l'intérieur », il a tous les droits.

La gestion correcte des accès repose sur six éléments :

1. **Gestion de l'identité :** tous les utilisateurs autorisés sont identifiés de manière standard. La gestion n'est toutefois pas toujours à jour, car les comptes dormants ne sont généralement pas supervisés et les comptes des anciens utilisateurs/employés ne sont pas fermés suffisamment rapidement, ce qui les laisse accessibles pour les accès non contrôlés.

2. **Gestion des droits** : en fonction des rôles couverts, les droits alloués permettent d'accéder à l'information, mais aussi de régir les activités ainsi que les créneaux horaires, et les lieux à partir

desquels les activités sont autorisées.

Cependant, de nombreuses PME accordent généralement l'accès sans gestion adéquate. Cela signifie que chacun a accès à tout, et même à distance, sans que l'entreprise puisse intervenir ou savoir qui a mal agi en cas de problème.

1. **Gestion de l'authentification :** tous les utilisateurs identifiés utilisent des identifiants dédiés pour accéder aux actifs et aux informations, selon leur niveau de classification.

La plupart du temps, le seul authentifiant est un mot de passe — généralement faible — qui n'est guère modifié… et valide pour tous les comptes et services. Cela signifie qu'une fois pris par un employé malhonnête ou un malfaiteur, ils ont accès à l'information de l'entreprise avec tous les droits.

2. **Contrôle d'accès :** les accès ne sont donnés que si l'identité, l'authentifiant et les droits correspondent.

C'est généralement plus ou moins bien.

3. **Enregistrement de l'événement :** tous les accès et tentatives sont enregistrés avec les détails du groupe date-heure (DTG), selon le niveau de classification. Les anomalies sont signalées au contrôleur/gestionnaire d'accès. Généralement, la taille du fichier est trop petite et, une fois la taille dépassée, le système commence à écrire sur les plus anciens, la plupart du temps seulement vieux de quelques jours. Les PME perdent ainsi beaucoup d'informations extrêmement importantes en cas d'incident.

4. **Analyse des logs** : les logs sont analysés régulièrement, et les comportements anormaux sont identifiés et contrés.

Cependant, la plupart des PME analysent à peine les registres, perdant de vue les événements qui peuvent indiquer au moins une tentative d'intrusion.

Si le contrôle d'accès est appliqué, même partiellement, sur les systèmes et les bâtiments TIC, les personnes non autorisées peuvent accéder à des informations protégées sans beaucoup de contrôle. Son application sur les bureaux et les salles est cependant plus épisodique. Les employés n'ont généralement pas accès aux bureaux (ils n'ont pas de clés) en dehors des heures d'ouverture. En outre, le nettoyage des bureaux se fait généralement en dehors des heures de travail, et les équipes de nettoyage ont accès à toutes les pièces, où l'information n'est pas toujours cachée.

Les règles générales concernant l'accès et l'utilisation de l'argent sont un bon exemple à appliquer à l'information.

Guidance

Les règles générales — et de base — qui suivent doivent être appliquées à la fois aux systèmes TIC et aux emplacements physiques sur une base continue. L'idée générale est que l'accès des utilisateurs (y compris des applications) à l'information, aux applications, aux services et aux salles est accordé à ce qui est strictement nécessaire pour effectuer le travail qui a été décidé.

- **Gestion de l'identité**
  - tous les utilisateurs internes et externes sont enregistrés de manière standard ;

- les comptes dormants concernant des utilisateurs temporairement inactifs sont gelés (droits et authentification bloqués et surtout surveillés) ;
- tous les membres du personnel et les utilisateurs qui ont quitté l'entreprise ont leur compte déconnecté pour éviter l'utilisation illicite et sont annulés après une période qui ne dépasse pas trois mois.

- **Gestion des droits**

  - droits à l'information concernant Lire, Écrire, Modifier, Copier, Transmettre/Communiquer (par exemple, par courriel), Imprimer.

Les droits sur les biens concernent l'Utilisation, la Maintenance, la Modification, le Déplacement (à l'intérieur et/ou à l'extérieur des installations de l'entreprise) ;

- les droits d'accès sont accordés pour exercer les activités en relation directe avec le rôle dans l'entreprise et la nécessité d'accéder et d'utiliser les informations. La relation avec la classification des informations (voir annexe A) est régulièrement vérifiée ;
- les rôles spéciaux tels que les administrateurs de système, les gestionnaires des RH, les analystes d'accès sont liés à des droits spéciaux (surveillance, etc.) ;
- les droits d'accès contiennent également des créneaux horaires autorisés et un emplacement autorisé (interne et/ou externe à l'entreprise) ;
- les droits sont régulièrement revus et adaptés en fonction de l'évolution des rôles dans l'entreprise.

- **Gestion de l'authentification**

  - il y a trois moyens d'authentification utilisés pour vérifier l'identité des utilisateurs autorisés : quelque chose que vous savez (mot de passe, code PIN…), quelque chose que vous possédez (une carte, une clé…) et quelque chose que vous êtes (empreintes digitales, dynamique de signature) ;
  - le choix du moyen d'authentification est fondé sur les tableaux de l'Annexe A ;
  - les mots de passe et les codes PIN sont régulièrement modifiés, en particulier lorsque l'utilisateur autorisé quitte l'entreprise ;
  - le mot de passe a une longueur minimale de huit caractères (majuscules et minuscules, figures et caractères spéciaux) et ne sera pas devinable par les autres utilisateurs.

- **Contrôle d'accès**

  - chaque tentative d'accès nécessite la présence à la fois de l'identifiant et de l'authentifiant associé et correspond aux horaires d'accès autorisés et à l'origine de l'accès ;
  - en cas de refus d'accès, le message indique que « les identifiants ne correspondent pas » ;
  - un maximum de tentatives est défini après quoi le compte sera gelé pour une période prédéfinie.

- **Journal d'événement**

- toutes les tentatives d'accès à l'information sont enregistrées avec le DTG ainsi que la source de la demande d'accès ;
- le fichier contient tous les enregistrements pour une période dédiée (au moins une semaine pour les accès autorisés et deux semaines pour les accès refusés) afin de permettre l'analyse.

- **Analyse des logs**
  - l'analyse des logs est associée à un rôle privilégié avec un compte spécial ;
  - des alarmes seront émises, par le biais des canaux de gestion des incidents, lorsque l'analyse montre des tentatives illicites présumées et lorsqu'un schéma prédéfini est découvert ;
  - les registres douteux seront sauvegardés (stockés en « lecture seule »[9]) de manière à ce qu'ils (1) ne puissent être perdus, (2) ne puissent être modifiés et (3) puissent servir de preuve en cas de réclamation ou de poursuite judiciaire.

Extension à la vie privée

L'accès et l'utilisation des données personnelles nécessitent un contrôle d'accès global qui respecte les règles énoncées dans les guidances ci-dessus.

13 CONTRÔLE #5 : SÉCURITÉ DU RÉSEAU ET ÉCHANGES DE DONNÉES

Contrôle

[9] La fonction « Lecture seule » (ROM : Read Only Memory) est une protection contre d'autres modifications.

Les PME devraient gérer et contrôler leurs réseaux afin de protéger les informations contenues dans les systèmes et les applications sur toutes les méthodes de connectivité.

Objectif

Assurer la protection de l'information dans les réseaux et les installations de traitement de l'information connexes.

Portée

Ce contrôle s'applique à la gestion de la sécurité de tous les dispositifs physiques et logiques qui font partie de l'infrastructure de réseau et de communication, des terminaux de connexion à Internet. Cela comprend les appareils mobiles (p. ex., les ordinateurs portatifs), les appareils personnels (p. ex., les smartphones), le Wi-Fi et les objets connectés (p. ex., les caméras de sécurité).

Situation

Il existe deux types de réseaux : le réseau local (LAN) et le réseau étendu (WAN). Le LAN est le réseau contrôlé par l'organisation, et le WAN est contrôlé par des forces extérieures à la nôtre. Le plus célèbre des réseaux WAN est l'Internet. La séparation entre LAN et WAN est connue sous le nom de périmètre.
Avant l'avènement d'Internet et des mobiles, le périmètre était un mur solide, difficile à percer pour les cybercriminels.

Cependant, maintenant, le périmètre est un peu flou. Les ordinateurs portables, smartphones et autres dispositifs amovibles quittent constamment le périmètre, établissant des connexions hors du contrôle de l'organisation. Parallèlement, le transfert d'information entre le réseau local et le réseau étendu est continu.

Guidance

Ci-après, nous soulignons les étapes les plus importantes pour mettre en œuvre un niveau de sécurité adéquat pour le réseau de nos organisations :

- **Établir et maintenir une politique de sécurité de la connectivité**. Cette politique tiendra compte du reste des points ci-dessous.
- **Les responsabilités et les procédures** de gestion des équipements de mise en réseau devraient être établies.
- **Ségrégation du réseau**. Il est nécessaire de diviser le réseau local (LAN) en sous-réseaux séparés, en fonction des besoins d'accès des utilisateurs, et d'appliquer la règle du moindre privilège. Les utilisateurs du domaine financier, par exemple, n'ont pas besoin d'accéder aux informations du domaine de la R&D. Si l'entreprise possède une zone de production, elle doit être séparée de la zone de gestion. L'isolement peut être physique ou virtuel. Les connexions entre les sous-réseaux peuvent être autorisées, mais doivent être contrôlées à l'aide d'une passerelle (pare-feu, routeur de filtrage, etc.). Par conséquent, le réseau devrait être segmenté autant que possible. Il est complexe, mais très important, **d'atteindre un équilibre** entre une bonne ségrégation du réseau et l'optimisation des opérations de l'organisation.
- La politique devrait déterminer si l'organisation permet aux appareils personnels utilisés pour des activités professionnelles, appelés BYOD (**Bring Your Own Device**), de se connecter au réseau. Ces appareils sont très dangereux parce qu'ils mêlent les questions personnelles et professionnelles, et parce qu'ils n'ont pas les mesures de sécurité minimale en place. Si autorisé, l'utilisateur doit

accepter d'appliquer certaines politiques et mesures de sécurité sur son appareil.

- Une architecture devrait exister montrant l'interconnexion des différentes **fonctions des équipements** du réseau et leur position par rapport au pare-feu (la passerelle protégée vers Internet).

- Mettre en œuvre **des mécanismes de filtrage réseau**, comme des pare-feus ou des logiciels de détection d'intrusion ; et appliquer les politiques de pare-feu pour contrôler le trafic entrant et sortant. Appliquez la règle de refus par défaut.

- Il devrait exister un schéma d'infrastructure indiquant les adresses IP internes, le système d'exploitation (SE) et le type de données hébergées.

- **Restreindre l'accès physique et logique** aux équipements réseau. Tous les systèmes sur les réseaux devraient être authentifiés et les systèmes connectés au réseau devraient être restreints. En outre, l'impossibilité de manipulation physique des équipements de réseau doit être assurée.

- Un utilisateur à l'extérieur du périmètre ne doit pas se connecter à **des routeurs WI-FI** qui ne sont pas sous son contrôle ou sous le contrôle de son organisation, car leur sécurité est particulièrement précaire. Il est beaucoup plus sûr de se connecter via téléphone mobile.

- La pandémie de COVID-19 a considérablement accru le **télétravail**. Cela signifie se connecter à notre réseau local (LAN) via un réseau public tel que l'Internet (WAN), afin de travailler. Utilisez un réseau privé virtuel (**VPN**) avec cryptage IPSec, si possible, pour les connexions de télétravailleurs. Pendant la pandémie, de nombreuses entreprises, surtout des PME, ont réduit leurs exigences de sécurité pour permettre le télétravail, ce qui a causé un plus grand nombre d'incidents de sécurité.

- **La journalisation et la surveillance** devraient être appliquées pour permettre l'enregistrement et la détection des actions qui peuvent affecter ou sont pertinentes pour la sécurité de l'information.

- Effectuer des tests de pénétration (« **pentests »**) périodiques pour déterminer si la protection du réseau est adéquate.

Extension à la vie privée

Une grande partie des informations qui transitent par les réseaux (LAN et WAN) peuvent être classées comme des données personnelles. Par conséquent, des contrôles spéciaux[10] doivent être en place pour assurer l'intégrité et la confidentialité de ces informations. La mesure la plus courante est le cryptage des communications, en évitant les attaques « *man in the middle* », qui consiste en une intrusion à n'importe quel point de la ligne de communication entre l'expéditeur et le récepteur, capturant les trames du réseau à travers les transferts d'information.

[10] Voir l'annexe A du Guide PME SBS pour la mise en œuvre de la norme ISO/IEC 27001 sur la gestion de la sécurité de l'information, p. 30 : 10.1.1. et 10.1.2

14 CONTRÔLE #6 : GESTION DES VULNÉRABILITÉS

Contrôle

Les PME devraient minimiser les risques résultant de l'exploitation malveillante de vulnérabilités connues. Il est donc essentiel de mettre en œuvre des mesures de protection pour éliminer ou contrôler les vulnérabilités, de tenir à jour une liste des vulnérabilités connues restantes et de sensibiliser le personnel des PME à ces vulnérabilités.

Objectif

Les PME minimisent la présence de vulnérabilités et permettent à leur personnel de faire preuve de prudence en matière de sécurité.

Portée

Sur la base de l'inventaire actuel et complet de la PME, la PME vérifie pour chaque actif TIC la mise en place de correctifs ou l'application d'autres mécanismes de protection. La priorité devrait être accordée aux actifs qui sont essentiels aux activités de la PME ou qui sont exposés à des menaces importantes et nouvelles (voir Veille des cybermenaces). Cela comprend le système d'exploitation.

Situation

De nouvelles vulnérabilités sont découvertes continuellement pour tout type d'actif numérique. Les fournisseurs publient des correctifs et des recommandations pour les vulnérabilités qui se font connaître pour leurs produits. De nombreuses PME n'en tiennent pas compte et travaillent encore, par exemple, avec des systèmes d'exploitation obsolètes et des applications qui ne sont plus maintenues, en raison de contraintes financières ou opérationnelles.

Guidance

Les vulnérabilités doivent être traitées au moins une fois par mois et lorsque des incidents ont été vécus par la PME. La gestion des vulnérabilités peut être effectuée par une personne désignée qui aide les utilisateurs des actifs à vérifier et à supprimer ou à contrôler les vulnérabilités.

La gestion des vulnérabilités est un processus en plusieurs étapes comportant une étape préliminaire et trois étapes qui devront être répétées régulièrement (au moins une fois par mois) ou lors d'un incident vécu par la PME.

1. **Identification des actifs numériques** : La PME doit créer un inventaire des actifs numériques (section 7.1) et, pour chaque actif, déterminer comment le fournisseur publie des correctifs ou des recommandations.

2. **Prioriser les actifs pour l'évaluation des vulnérabilités** : La PME devrait prioriser l'inventaire des actifs pour la criticité métier de l'actif et l'exposition de l'actif aux menaces nouvelles ou critiques (voir contrôle Surveillance des cybermenaces).

3. **Appliquer les correctifs et autres mécanismes de protection sur les actifs TIC :** Chaque actif doit être vérifié pour la présence de nouveaux correctifs ou de recommandations. Il convient de vérifier si ces correctifs impliquent des risques ou des coûts que la PME ne peut supporter et les vérifier avant de les installer sur tous les actifs du même type. Des correctifs acceptables doivent être installés. Pour les fournisseurs de confiance et lorsque des backups des actifs concernés sont disponibles, le correctif peut être automatisé. Les actifs qui ne peuvent pas être corrigés devraient être protégés par d'autres moyens, désactivés, protégés par des contrôles d'accès comme des pare-feu ou surveillés de près.

4. **Communiquer les vulnérabilités restantes :** La PME doit suivre les progrès de la correction dans l'inventaire des actifs numériques. Il doit informer le personnel sur les actifs non corrigés et proposer des recommandations pour une interaction sûre ou prudente avec ces actifs.

5. **Mettre en œuvre périodiquement les correctifs et les recommandations :** Les correctifs et les recommandations devraient être mis en œuvre par la PME le plus rapidement possible si l'avantage de protection l'emporte sur les risques associés à la fermeture de la vulnérabilité.

Cependant, les PME mettent rarement ces correctifs en œuvre de façon cohérente. Il est recommandé aux PME de partager leurs expériences avec d'autres PME. Au sein d'une telle communauté de pratique, les PME peuvent tirer profit les unes des autres pour améliorer l'efficience et l'efficacité de leur gestion des vulnérabilités et partager des conseils concernant les actifs ou les correctifs problématiques.

Extension à la vie privée

Lors de l'évaluation des vulnérabilités, la PME devrait prioriser les actifs utilisés pour gérer l'information représentant les clients et les utilisateurs.

15 CONTRÔLE #7 : LUTTE CONTRE LES LOGICIELS MALVEILLANTS

Contrôle

Les PME devraient mettre en œuvre et tenir à jour une politique et des outils appropriés pour contrer les logiciels malveillants.

Objectif

Pour rester protégé contre les dommages les logiciels malveillants peuvent causer aux systèmes TIC, aux processus opérationnels et aux objectifs.

Portée

Les malwares sont beaucoup plus complexes que ne le pensent les PME et les individus. Ces malwares se propagent dans le système informatique par :

- un dossier ou un contact infecté ;
- un courriel d'hameçonnage ;
- l'agence ou l'action d'un pirate informatique ;
- visiter un site Web infecté (ou malveillant).

Quel que soit le type et le mode d'infection, les effets vont de bénins à extrêmement graves.

Situation

De la même façon, comme les particuliers, les PME ne prêtent guère attention à la vaste gamme de modes d'infection par les logiciels malveillants et considèrent l'acquisition et la mise à jour régulière[11] d'un logiciel « antivirus » suffisant. La plupart du temps, ils conservent la même solution pendant des décennies.

Guidance

Les PME devraient :

- revoir régulièrement leur politique anti-malware pour la tenir à jour avec l'environnement de menace et le contexte commercial/technologique ; cela signifie vérifier auprès d'experts et de sites fiables les meilleures solutions, car l'efficacité varie au fil du temps ;
- s'assurer que tous les ordinateurs sont protégés en permanence ;
- installer sur les ordinateurs, les serveurs et les nœuds de communication des technologies de solutions anti-malware différentes – pour permettre des capacités de détection croisée ;
- vérifier que leur programme de sensibilisation à la sécurité revient régulièrement sur le drill anti-phishing afin que les employés et les utilisateurs ne tombent pas dans les ruses du pirate ;
- analyser régulièrement la situation des cybermenaces à l'aide de rapports publics/privés — voir Annexe D — ou en consultant un organisme spécialisé et revoir leur préparation.

Extension à la vie privée

Aucun problème particulier lié à la protection de la vie privée.

16 CONTRÔLE #8 : GESTION DES BACKUPS

Contrôle

Des copies de sauvegarde des informations, des logiciels et des images du système doivent être prises et testées régulièrement conformément à une politique convenue.

Objectif

L'information est l'actif le plus précieux d'une entreprise. Par conséquent, il est nécessaire d'avoir des copies qui assurent leur disponibilité, leur intégrité et leur confidentialité.

Portée

[11] Le groupe d'experts européen de la sécurité informatique fournit des informations actualisées sur les solutions antivirus. En outre, la plupart des solutions antivirus ou de sécurité fournissent une liste des derniers logiciels malveillants/spyware/chevaux de Troie.

Ce contrôle s'applique à toutes les informations, logiciels et configurations de systèmes de l'organisation.

Situation

Différents risques menacent les informations détenues par les organisations (ransomware et autres attaques de cybercriminels, pannes de matériel ou de logiciel, erreurs humaines, incendies, inondations, etc.). Cependant, en de nombreuses occasions, nous continuons à trouver un manque de backups, ou des copies faites d'une mauvaise manière, à partir de laquelle il est impossible de récupérer le contenu.
En outre, pour forcer le paiement pour récupérer l'information, les cybercriminels tentent d'éliminer les copies de sauvegarde avant de procéder à crypter l'information à l'aide du ransomware. Il devient donc essentiel d'avoir une copie hors site.

Guidance

Une politique de backups devrait être élaborée pour établir les exigences de l'organisation en matière de sauvegarde des informations, des logiciels et des configurations. De plus, la politique de conservation et les exigences de protection de sauvegarde doivent être définies pour chaque type d'information.
Pour la procédure de sauvegarde, nous recommandons d'utiliser la stratégie de sauvegarde 3-2-1 :

- (3) Conserver au moins 3 copies de vos données.
- (2) Conserver deux exemplaires à des endroits distincts.
- (1) Entreposer au moins 1 exemplaire à un endroit hors site.

Une copie contient les données de production, les deux autres copies sont des backups. Chacune de ces copies devrait contenir la même version des données, prise au même moment. Au moins une copie doit se trouver à un autre endroit, à une distance suffisante pour être à l'abri d'une catastrophe sur le site principal.

Les informations sauvegardées devraient être protégées de façon appropriée sur les plans physique et environnemental, conformément aux normes appliquées sur le site principal (voir le contrôle #9 : Gestion des mesures de protection, ci-dessous). Tous les backups doivent être chiffrés. L'accès au logiciel de sauvegarde et au stockage doit être protégé par des identifiants d'administration spécifiques.
Les journaux de sauvegarde doivent être examinés quotidiennement pour vérifier si les copies ont été remplies correctement ou si des erreurs se sont produites.

Toutes les informations d'une organisation ne sont pas aussi importantes pour l'entreprise[12]. Pour cette raison, des plans de backups doivent être conçus pour optimiser le processus en fonction des exigences de sécurité de l'information.

Selon le type d'information, l'existence de différentes politiques de conservation est l'un des points les plus

[12] Les considérations de coût jouent également un rôle ici. Par exemple, l'entreprise doit copier les changements à la base de données ERP tous les jours, mais les photos du dernier congrès une fois par an. Si l'entreprise a une copie dans le cloud, le coût pourrait être important.

complexes lors de la conception de plans de backups. Puisque les politiques de conservation s'appliquent également aux informations stockées dans les sauvegardes, il est généralement nécessaire de configurer différents plans de backups en fonction des différentes périodes de conservation.

Enfin, des tests de restauration devraient être effectués périodiquement sur les sauvegardes effectuées afin de s'assurer que les informations peuvent être restaurées si nécessaire.

Extension à la vie privée

Dans la plupart des cas, les copies de sauvegarde contiennent des données personnelles, il est donc particulièrement important que les copies soient stockées cryptées et que les périodes de conservation[11] établies pour se conformer au RGPD soient respectées[13].

17 CONTRÔLE #9 : GESTION DES MESURES DE PROTECTION

Contrôle

Les PME devraient protéger les informations importantes et les actifs numériques contre la perte, la destruction et la falsification. La protection comprend la planification, la création et les essais répétés. Une protection particulière est les backups[14].

Objectif

Les PME devraient protéger les informations importantes et les actifs numériques contre la perte, la destruction et la falsification.

Portée

Sur la base de son inventaire d'actifs numériques, la PME planifie, crée et teste à plusieurs reprises des mesures de protection. Les mesures de protection du matériel comprennent l'utilisation de salles ou d'armoires verrouillées et l'utilisation de systèmes antivol. Les mesures de protection des logiciels et de l'information comprennent l'authentification, p. ex., avec des mots de passe forts et une authentification à deux facteurs, le chiffrement du stockage et de la transmission des données, p. ex., avec un système de VPN, et la protection des actifs numériques par des mesures anti-logiciels malveillants, pare-feu et journalisation du système. Le personnel qui gère les mesures de protection et celui qui a accès à des informations secrètes ou personnelles devrait être contrôlé quant à sa fiabilité. Les backups doivent être créés à intervalles réguliers et leur récupération testée.

Situation

De nombreux types d'attaques ciblent l'accès non autorisé, l'écoute clandestine, la falsification et le vol d'information. En outre, les actifs numériques peuvent casser ou devenir inutilisables pour diverses raisons. Des mesures de protection sont établies pour protéger contre de tels types de menaces.

[13] Les durées de conservation dépendent des secteurs, des lois applicables, du type d'information, des contrats avec les clients et d'autres facteurs. Il n'y a pas de règles définies pour tous.
[14] Reportez-vous au contrôle #8 : Gestion des backups.

Guidance

La gestion des mesures de protection est un processus en plusieurs étapes contenant :

1. **Identification des actifs numériques** : La PME doit créer un inventaire des actifs numériques (section 7.1) et, pour chaque actif, déterminer son importance opérationnelle. La PME devrait prioriser l'inventaire des actifs pour la criticité métier de l'actif et l'exposition de l'actif aux menaces nouvelles ou critiques (voir contrôle Surveillance des cybermenaces).

2. **Protection de l'accès aux actifs numériques** : La PME devrait déterminer comment chacun des actifs numériques doit être protégé. Cela comprend : les garanties physiques pour le matériel ; les garanties numériques pour les logiciels (p. ex., avec contrôle d'accès avec mots de passe forts ou authentification à deux facteurs, protection des terminaux avec anti-malware) ; les réseaux (p. ex., avec cryptage et pare-feu) et les données (p. ex., stockage et transmission cryptés et utilisation d'un VPN).

3. **Protection contre la perte d'informations et de logiciels** : la PME devrait créer un backup à jour des systèmes et de l'information critique pour l'entreprise. Les backups doivent être identifiés et datés, et la capacité de récupérer les systèmes et les informations testée.

4. **Prévision des mesures de protection propres à chaque menace :** Pour chaque menace nouvelle ou critique, la PME devrait consulter les recommandations visant à prévenir et à se défendre des attaques. Les CERT qui fournissent de l'information sur les menaces offrent souvent de telles recommandations.

5. **Établissement de la confiance :** La PME devrait vérifier la fiabilité du personnel technique et du personnel ayant accès aux renseignements essentiels.

6. **Établissement d'une solide culture de sécurité :** La PME devrait informer tout le personnel au sujet des comportements sécuritaires ou prudents. Cela comprend : la façon de travailler avec les backups et leur récupération ; la façon d'utiliser les actifs commerciaux essentiels ; la façon de protéger l'accès aux actifs (p. ex., en utilisant des mots de passe uniques et forts ou l'authentification à deux facteurs). Une solide culture de sécurité comprend également la formation du personnel pour détecter les attaques, p. ex. fondée sur diverses formes d'hameçonnage et d'ingénierie sociale.

Extension à la vie privée

Le RGPD exige que la PME assure la sécurité appropriée des données à caractère personnel, y compris la protection contre les traitements non autorisés ou illégaux et contre les pertes, destructions ou dommages accidentels. L'expert en la matière doit désigner une personne, le « contrôleur », qui est responsable de la protection et de la conformité.

18 CONTRÔLE #10 : PRÉPARATION[15] DES TIC À LA CONTINUITÉ DES ACTIVITÉS

Contrôle

Les systèmes de TIC devraient être conçus (sécurité par conception et par défaut) pour résister et être résilients aux défaillances et aux problèmes.

Objectif

Les PME sont confiantes que les défaillances et les problèmes des TIC n'auront pas d'effets négatifs graves sur les processus, les objectifs et les enjeux de l'entreprise.

Portée

Ce contrôle couvre les systèmes TIC et les installations physiques qui leur permettent de fonctionner (p. ex., l'électricité, la climatisation, un toit et des personnes qualifiées).

[15] En fait, être fin prêt à…

Situation

Quelles qu'en soient la cause, les situations imprévues mettent à l'épreuve la compétitivité et les capacités d'une entreprise. Si une entreprise gère efficacement les crises, sa valeur marchande et sa réputation peuvent prospérer. Ainsi, il est crucial pour une entreprise d'être prête pour la continuité des activités, en particulier du point de vue des TIC.

Un plan de continuité des activités (PCA ou BCP) contribue à rendre les entreprises aussi résilientes que possible, car il peut :

- limiter les interruptions (moins de temps d'arrêt, moins d'argent perdu) ;
- présenter des solutions de rechange (pour relancer rapidement les activités) ;
- habiliter les employés.

Guidance

Chaque entreprise reçoit rarement un préavis qu'une cyberattaque est prête à frapper, et beaucoup pensent que chaque incident est unique et se déroule de manière attendue.
Si un entrepreneur ou un cadre supérieur veut donner à son organisation la meilleure chance de réussir en cas de catastrophe, il doit mettre à jour un plan, éprouvé entre les mains de tout le personnel responsable de l'exécution de toute partie de ce plan ; toutefois, avant de parler de plans, de mesures et de mesures correctives, il est important de se concentrer sur les trois principaux piliers et les cinq principes de la continuité des activités.
Les trois piliers sont : culture/sensibilisation de l'entreprise ; politiques ; technologie.

Culture et sensibilisation de l'entreprise

La prise de conscience est fondamentale pour intégrer la pratique de continuité des activités dans les activités de l'entreprise, et changer la culture de l'organisation est la chose la plus difficile à faire, car il faut beaucoup de temps pour la mettre en œuvre.
En général, voici les étapes que toute organisation devrait suivre pour accroître sa culture de continuité des activités :

1. Commencez par la direction. Il peut parfois être difficile de communiquer avec la haute direction. Toutefois, c'est essentiel parce que le changement de continuité des activités se produit par une approche descendante (top-down). Commencez par introduire des concepts de continuité d'activité et montrer les avantages à long terme, en particulier d'un point de vue financier.
2. Formez une équipe d'influenceurs qui comprennent les avantages et aident à renforcer la résilience de l'entreprise.
3. Utilisez toujours une approche collaborative pour amener tous les employés à essayer d'améliorer ou de changer la culture d'entreprise.
4. Investissez dans la formation, y compris les webinaires, les livres blancs et les documents d'information. Nous vous recommandons de répéter les simulations trois fois par an et rappelez-vous que la continuité des activités n'est pas une image unique, mais un film sans fin !

Politiques

Des politiques de continuité d'activité sont créées pour renforcer l'organisation de l'entreprise, en respectant les exigences du marché et de conformité. Ils documentent ce qui est nécessaire pour maintenir

une organisation en activité les jours ouvrables ordinaires ainsi que pendant un incident. Lorsque les politiques sont bien définies et clairement respectées, l'organisation peut établir des attentes réalistes en matière de continuité des activités et des processus. Les politiques servent également à mesurer ce qui a mal tourné pendant une crise, à améliorer la résilience de l'entreprise et à régler les problèmes.

L'une des principales choses à considérer lors de l'élaboration d'une politique de continuité des activités est les risques particuliers auxquels une organisation est susceptible de faire face. En ce qui concerne l'état de préparation des TIC, la première question à se poser est la suivante : y a-t-il eu des problèmes liés aux incidents de TIC par le passé qui nécessitent une attention particulière ? La comptabilisation de tous ces facteurs pourrait aider à créer de bonnes politiques.

La colonne vertébrale d'une politique de continuité des activités repose sur l'analyse des impacts sur les activités (BIA) et l'évaluation des risques.

Un BIA établit les effets d'une catastrophe potentielle sur une organisation en trouvant les vulnérabilités existantes et se concentre principalement sur les impacts sur les activités, le temps de reprise (RTO) et les objectifs de points de reprise (RPO).

L'autre méthode fiable pour découvrir les menaces potentielles consiste à déterminer leur vraisemblance au moyen d'une évaluation des risques afin de cerner les dangers et de trouver des façons de réduire leur incidence sur les activités et de réduire rapidement le temps nécessaire pour établir la nouvelle normalité après un incident. Une évaluation des risques devrait aider à :

- identifier les dangers ;
- évaluer les risques ;
- créer des mesures de contrôle ;
- consigner les constatations ;
- surveiller les améliorations.

Technologie

Une fois qu'une organisation a développé sa culture et ses politiques, il est temps de penser aux technologies qui peuvent aider à construire une meilleure résilience.

Même si les organisations disposent de budgets modestes en matière de cybersécurité, elles prêtent attention à leur consommation de ressources, car celles-ci ont de grandes chances d'être ciblées par la cybercriminalité. Ainsi, pour renforcer l'état de préparation du plan de continuité des activités, nous devons commencer à obtenir deux atouts importants :

- Utilisateurs
- Environnement

Plan de continuité des activités

Le principal objectif d'un plan de continuité des activités est de préserver les ressources humaines, de protéger les biens et de maintenir les activités le plus possible en cas de crise afin que les activités normales puissent reprendre le plus tôt possible.
Se basant sur l'évaluation, la préparation, l'intervention et le rétablissement, un plan de continuité des activités assurera :

- engagement humain
- qualité
- croissance
- satisfaction du client.

Pourquoi une organisation a-t-elle besoin d'un PCA ?

« Ça ne nous arrivera pas » est la chose la plus facile à dire et à penser quand une catastrophe ne semble pas être à l'horizon. Cependant, les catastrophes n'ont pas de frontières et si une crise se produit ou pas, c'est une bonne idée d'être préparé avec un plan pour aider votre entreprise à réagir. Soyez prêt pour l'inconnu et rappelez-vous : si vous pouvez gérer un problème, vous serez en mesure de l'aborder et d'évaluer ce qui se passe, et quand vous reviendrez à la normale.

Lorsqu'un incident informatique survient, les clients, les employés et les partenaires doivent savoir qu'ils sont protégés et qu'on prendra soin d'eux. Le PCA couvrira tout au sein de l'entreprise et établira la réputation de votre entreprise.

Comment établir un plan de continuité des activités

Tout d'abord, rappelez-vous qu'un PCA doit se concentrer sur ces trois facteurs clés :

- Résilience ;
- Redressement ;
- Contingence.

Dès lors, que devrait comprendre un plan de continuité des activités ? La bonne réponse est que cela dépend de la catastrophe.

Dans un monde parfait, vous devriez avoir des plans personnalisés pour chaque problème potentiel. La façon de traiter un problème de réseau ne sera pas identique à la façon dont vous réagissez à une pandémie et le processus de rétablissement ne sera pas le même non plus.

1. **Identifiez les risques**

Commencez à vous poser des questions comme :

- Comment le personnel se rendra-t-il au bureau ?
- S'ils ne peuvent pas s'y rendre, travailleront-ils à distance ?
- Avez-vous besoin de leur envoyer du matériel pour qu'ils puissent travailler de la maison ?
- Où placerez-vous le personnel qui peut entrer dans les bureaux ?
- Comment allez-vous communiquer avec le personnel, les membres du conseil d'administration, et les clients au sujet de la catastrophe/les dommages ?
- Devrez-vous remplacer quoi que ce soit après cette catastrophe ?
- Avez-vous le budget nécessaire pour remplacer des choses et éventuellement créer un autre bureau ?

Ces questions vous donneront une idée très simple de la façon dont votre entreprise pourrait être touchée et de la façon dont vous devrez réagir à cette perturbation.

2. **Décidez de ce que vous devez protéger**

Déterminez ce que vous devez protéger et où vous pourriez être le plus vulnérable. Pensez aux renseignements qui pourraient se trouver à l'intérieur du bureau et réfléchissez à la façon de les protéger même s'ils ne sont pas numériques. Pensez au personnel, n'oubliez pas qu'il aide à maintenir l'entreprise active. Réfléchissez à la façon dont ils continueront de travailler. Examinez les processus et les politiques. Vous devez protéger vos opérations et vos services pour le bien de l'entreprise et des clients qui les utilisent.

3. **Déterminez les mesures de gestion des risques**

Évaluez les mesures actuellement en place et celles qui pourraient manquer.

4. **Créez votre ou vos plans**

Réfléchissez plus en détail à la façon dont vous allez organiser le personnel, protéger les bureaux et vous assurer que l'entreprise dans son ensemble se portera bien pendant cette période. Ces plans couvrent la sécurité, la sûreté et les plans généraux pour protéger l'entreprise.

5. **Pratiquez et pratiquez à nouveau !**

Ne laissez pas votre plan dans un tiroir. Nous recommandons de planifier des tests deux fois par an. L'expérience est précieuse. Utilisez votre pire scénario et titrez en des pratiques exemplaires.

Pratiquer vous donnera l'occasion de voir l'efficacité de votre plan. Cela est particulièrement utile si vous manquez quelque chose ou si quelque chose ne va vraiment pas fonctionner et doit être planifié d'une meilleure façon. Demandez des commentaires aux employés, aux clients et aux fournisseurs.

Pourquoi les entreprises ont-elles besoin d'une analyse d'impacts sur les activités (BIA) ?

Un BIA vous aide à déterminer et à documenter les processus opérationnels essentiels et leurs éléments de soutien. Cela aide à comprendre votre environnement, et ce qui est le plus important, avant de prendre des mesures pour le protéger. Le BIA révèle comment ces activités et fonctions clés auraient une incidence sur la continuité des activités si elles étaient entravées ou éliminées.

Qu'est-ce que le BIA permet ?

- Déterminer les principaux processus et fonctions opérationnels.
- Établir les priorités, les processus opérationnels et les fonctions.
- Établir une liste détaillée des exigences pour la reprise des activités.
- Déterminer l'impact sur les opérations quotidiennes.
- Élaborer les exigences en matière de temps de récupération.
- Déterminer les répercussions financières, opérationnelles et juridiques des perturbations.

Comment effectuer une analyse d'impact sur les activités (BIA) ?

- La première étape de la réalisation d'un BIA réussie consiste à s'assurer que les bonnes activités et ressources opérationnelles entrent dans le périmètre. Une fois que les produits et services sont considérés comme faisant partie du champ d'application, les départements requis devraient être identifiés aux fins d'inclusion dans le processus de BIA.
- Après avoir déterminé les services et les activités visés, planifiez des réunions avec les dirigeants de chaque département. Pour obtenir un meilleur résultat, tous les participants doivent :
  - connaître les priorités clés de l'organisation (puisqu'elles concernent les produits et services) ;
  - comprendre les activités quotidiennes du département ;
  - comprendre les dépendances des ressources nécessaires pour mener à bien chaque activité opérationnelle.
- Réalisez des entretiens BIA et d'évaluation des risques afin de déterminer les activités du département qui appuient la production des produits et services visés. Pour chaque activité, il est important de fixer toutes les étapes nécessaires pour mener à bien l'activité, les périodes de pointe, les répercussions des temps d'arrêt (c'est à dire financières, de réputation, opérationnelles) et les dépendances nécessaires pour exécuter chaque activité. Nous suggérons de documenter les types de dépendance suivants :
  - Applications

- Installations
- Fournisseurs tiers
- Équipement
- Personnel

• Documentez et approuvez le rapport de BIA de chaque département avec les résultats de la réunion. Ces rapports devraient contenir tous les renseignements et recommandations recueillis au cours de chaque entretien.

• Remplissez un résumé du BIA pour l'examen et l'approbation par la direction. Cette tâche vise à donner un aperçu des principales activités, des besoins en ressources et des risques cernés au cours des réunions de niveau inférieur.

19 CONTRÔLE #11 : TÉLÉTRAVAIL

Contrôle

Une politique et des mesures de sécurité connexes devraient être mises en œuvre pour protéger l'information consultée, traitée ou stockée sur les sites de télétravail.

Objectif

Le travail à distance est de plus en plus courant et oblige les entreprises à mettre en place des mesures de sécurité spécifiques pour un environnement où le périmètre est de plus en plus diffus. Ces mesures protégeront l'entreprise contre le vol d'information et l'intrusion illicite dans ses systèmes TIC par les canaux de communication et l'utilisation inappropriée des ordinateurs qui sont hors de leur contrôle.

Portée

Ce contrôle s'applique chaque fois que les utilisateurs travaillent à partir d'un endroit à l'extérieur du bureau où ils développent régulièrement leurs activités.

Situation

Le travail à distance a connu une croissance progressive ces dernières années. Toutefois, en raison de la pandémie de COVID-19 et du confinement qui en a découlé, la nécessité de fournir à tous les travailleurs l'équipement nécessaire et les droits d'accès permettant le travail à la maison a amené les entreprises à assouplir les mesures de sécurité pour faciliter le travail à distance.

Les cybercriminels ont profité de la situation pour déployer toutes sortes de mécanismes qui leur permettent d'obtenir des renseignements sur les utilisateurs, de détourner des informations, de mener des attaques ciblées, etc.

Dans l'après-pandémie, le télétravail ne reviendra pas à la situation antérieure, mais devrait être de plus en plus important dans le développement des activités commerciales.

Guidance

Voici les étapes les plus importantes pour mettre en œuvre un niveau de sécurité adéquat pour le travail à distance :

- Définissez, approuvez et diffusez une politique de sécurité spécifique pour le travail à distance. Cette politique envisagera l'utilisation appropriée des médias de l'entreprise et couvrira toutes les variables possibles, telles que: l'utilisation ou non d'ordinateurs domestiques et la possibilité d'y accéder pour vérifier la sécurisation de l'équipement; le besoin de licences logicielles; les exigences relatives aux lignes de communication; la sécurité du lieu de travail et la préservation de la confidentialité, etc.
- Dans la mesure du possible, l'équipement utilisé pour le télétravail devrait être un ordinateur d'entreprise, et l'utilisateur ne devrait jamais l'utiliser à des fins personnelles. Par conséquent, les utilisateurs ne devraient pas utiliser des ordinateurs domestiques pour des affaires professionnelles.
- Les utilisateurs doivent se connecter uniquement aux réseaux Wi-Fi sous leur contrôle et avec la sécurité de type WPA2.
- L'entreprise doit définir et configurer la protection des terminaux pour les travailleurs à distance, et s'assurer qu'elle est active et à jour.
- De plus, le système d'exploitation doit toujours être à jour.
- L'équipement de l'entreprise fourni pour le travail à distance, habituellement les ordinateurs portatifs, doit être chiffré.
- Les canaux de vidéoconférence doivent être chiffrés.
- Fournir une connectivité via un VPN sécurisé, en utilisant le protocole IPSec si possible.
- Éviter d'utiliser les connexions de bureau à distance, car elles sont l'un des principaux vecteurs d'attaque.
- Si possible, l'authentification à deux facteurs devrait être mise en œuvre.
- L'utilisateur doit s'assurer que son travail est stocké dans les systèmes de l'entreprise. Une erreur courante lors du travail à distance est d'enregistrer les documents de travail localement, qu'ils ne peuvent pas, ainsi, être inclus dans les sauvegardes configurées par l'entreprise.
- N'assouplissez pas les mesures de sécurité pour faciliter le travail à distance.
- Assurez-vous de révoquer les droits d'accès et de retourner l'équipement lorsque le travail à distance est terminé.

- Formez le personnel pour empêcher l'accès abusif à l'équipement et aux données en les protégeant dans une armoire fermée.
- Formez le personnel pour qu'il évite de travailler sur des « informations protégées » (voir la section 7.3 : Gestion des biens) pendant que des personnes non autorisées rôdent aux alentours.

Extension à la vie privée

Lors du travail à distance, les informations personnelles passent par des réseaux externes jusqu'à ce qu'ils atteignent le réseau de l'entreprise. Il est donc très important d'utiliser les connexions VPN. En outre, dans un environnement domestique, une attention particulière doit être accordée à la confidentialité des informations.

20 CONTRÔLE #12 : SURVEILLANCE DES CYBERMENACES

Contrôle

Les menaces nouvelles et émergentes mettent les PME au défi d'adapter leurs pratiques de sécurité pour demeurer continuellement protégées. Il est donc crucial d'observer les changements dans le paysage de la menace.

Objectif

Les PME sont protégées contre les menaces nouvelles et émergentes en tirant leur besoin de contrôles de sécurité d'une compréhension à jour du contexte des menaces.

Portée

Les contrôles de sécurité sont mis en œuvre en fonction des risques découlant des menaces. Par conséquent, les risques doivent être évalués chaque fois que de nouvelles menaces sont identifiées. La portée de ce contrôle est l'identification des menaces pour l'évaluation et la planification de l'atténuation des risques. La gestion des risques sera soumise à d'autres contrôles.

Situation

Un large éventail de menaces représente des risques pour la sécurité de l'information qui peuvent nuire à la continuité de vos activités. Alors que les grandes catégories de menaces sont restées stables au cours de la dernière décennie, de nouvelles attaques sont inventées et essayées en permanence. De plus, ces menaces diffèrent selon l'emplacement géographique et le secteur d'activité de l'entreprise.

Guidance

La surveillance des cybermenaces est un processus en quatre étapes comportant une étape préliminaire et trois étapes qui devront être répétées régulièrement :

1. **Identification des sources** : La PME doit identifier toutes les sources d'information sur les menaces à consulter lorsqu'elle prend connaissance de nouvelles menaces. Ces sources peuvent inclure des publications et des rapports de groupes d'intérêts spéciaux, d'organismes de cybersécurité comme les CERT nationaux, d'entreprises de confiance et de médias spécialisés dans la surveillance des

menaces.

2. **Identifiez les nouvelles menaces :** Lorsque vous consultez une source, les nouvelles menaces doivent être documentées. Les menaces peuvent être marquées comme n'étant pas applicables/pertinentes si une justification est donnée à cet effet.
3. **Déterminez l'incidence sur l'évaluation des risques** : Les menaces identifiées doivent être intégrées à l'évaluation des risques pour déterminer si elles entraînent de nouveaux risques inacceptables.
4. **Planification des mesures de traitement :** Si de nouveaux risques inacceptables découlent de la troisième étape, des mesures appropriées doivent être prévues pour atténuer ces risques.

Il est important de comprendre que la surveillance des cybermenaces est une activité à répéter à intervalles réguliers. Pour la PME, il est important d'être au courant des menaces importantes et de rester au courant en cherchant de nouvelles menaces tous les trois mois.
Pour l'identification des sources d'information sur les nouvelles menaces, un cycle annuel peut être utilisé.
En outre, des attaques spécifiques telles que l'arnaque Flubot peuvent affecter une PME dans les heures suivant sa première apparition, appelant à une action immédiate, p. ex. un avertissement sur les canaux de communication interne de l'entreprise. Les bulletins d'informations peuvent fournir des avertissements précoces et agir selon les recommandations de confiance se traduira par une réponse en temps opportun.

1. Identification des sources d'information : Les sources typiques comprennent les groupes d'intérêts spéciaux, les agences de cybersécurité comme les CERT nationales, les entreprises de confiance et les médias spécialisés dans la surveillance des menaces. Exemples :

- L'ENISA rassemble et publie des informations sur les menaces pour l'ensemble de l'Europe environ une fois par an. Ces publications offrent un aperçu général et grossier du paysage de la menace.
  - Aperçu des publications
  - Principales menaces pour 2020
- Dans chaque État membre de l'UE et dans d'autres pays européens, des centres officiels de cybersécurité[16] ont été créés. Pour les PME, elles offrent des rapports à jour, des recommandations et des abonnements locaux sur les menaces. Les points suivants peuvent être utiles pour les menaces propres aux PME, surtout compte tenu de leur emplacement. Un exemple de CERT avec des informations pour les PME[1] :
  - Roumanie, Directoratul National de Securitate Cibernetica
  - Suisse, National Cybersecurity Centre (NCSC)
  - Pays-Bas, Dutch Digital Trust Centre

2. Identifier les nouvelles menaces : Les nouvelles menaces doivent être documentées et utilisées pour réduire le temps nécessaire à l'évaluation des risques. Les menaces qui ne s'appliquent pas à la PME devraient être incluses dans la documentation et

[16] L'ENISA a publié un rapport sur les CERT avec des recommandations sur les capacités de base. 14 L'annexe D contient une liste complète des CERT dans les États membres + Royaume-Uni

accompagnées d'une justification de leur non-prise en compte.

3. **Déterminer l'impact sur l'évaluation des risques** : Dès qu'une nouvelle menace est identifiée, la PME devrait revoir son évaluation des risques pour assurer une protection adéquate. Un ou plusieurs risques peuvent être ajoutés pour chaque actif auquel la menace pourrait s'appliquer. Si un risque similaire est déjà mentionné, sa vraisemblance et son impact doivent être révisés.

4. **Planification des mesures de traitement** : Après l'évaluation des risques, les cotes de risque doivent être évaluées. Pour les nouveaux risques, l'introduction de nouveaux contrôles de sécurité peut être appropriée pour ramener le risque à un niveau acceptable. Pour les risques qui ont été modifiés en raison d'une nouvelle menace, la vraisemblance et l'incidence peuvent avoir augmenté la cote de risque. Par conséquent, la PME pourrait devoir adapter ses contrôles de sécurité. Les contrôles de sécurité nouveaux et adaptés devraient être priorisés et planifiés pour leur mise en œuvre.

Extension à la vie privée

Lors de l'évaluation des menaces pendant l'évaluation des risques, la PME devrait tenir compte de l'incidence sur la disponibilité, l'intégrité et la confidentialité de l'information. Pour protéger la vie privée, il faut porter une attention particulière aux biens contenant des informations personnelles et aux menaces qui pourraient avoir une incidence sur la confidentialité des informations contenues dans ce bien (voir Contrôle #1 : Gestion des biens).

21 CONTRÔLE #13 : SENSIBILISATION À LA SÉCURITÉ DE L'INFORMATION

Contrôle

Le personnel et les utilisateurs des systèmes d'information et des TIC devraient être informés des objectifs et des règles de sécurité de l'information. Les attentes doivent être claires et comprises. Le personnel ayant des rôles précis devrait être formé pour accomplir ses tâches.

Objectif

Les PME sont confiantes que leur personnel et leurs utilisateurs respectent les objectifs de sécurité de l'information et se comportent comme prévu dans la plupart des cas.

Portée

Ce contrôle s'applique à toutes les informations traitées par l'entreprise, ainsi qu'aux systèmes et applications informatiques qui donnent accès et permettent le traitement des informations commerciales et connexes. Cela comprend les informations financières et privées.

Situation

Il y a quatre niveaux de communication de l'information :

1. **Informé :** À ce sujet, les gens disent qu'il y a quelque chose de disponible quelque part : c'est similaire aux journaux d'information. Personne n'est obligé

de les lire et de les appliquer. En ce qui concerne la sécurité de l'information, cette option n'est pas pertinente et ne devrait pas être choisie.

2. Conscient : En utilisant ce mode de communication, le personnel et les utilisateurs sont forcés de lire et devraient prendre conscience de la question, les objectifs ainsi que leur rôle et responsabilité. Comme bon nombre de ces changements sont fréquents — c.-à-d. les objectifs et les processus opérationnels, les menaces à l'information, les solutions disponibles —, les séances (et les programmes) de sensibilisation devraient être répétées régulièrement.

3. Formé : Avec ce mode de communication, les personnes qui ont un rôle spécifique ou qui doivent acquérir une nouvelle attitude, une nouvelle habitude ou une nouvelle compétence reçoivent tout ce dont elles ont besoin pour faire ce qu'on attend d'elles.

4. Instruit : Il s'agit du modèle de communication le plus élevé dans lequel le personnel impliqué obtient un supplément d'information afin qu'il sache le cheminement de la réflexion sécuritaire, dit autrement pour comprendre pourquoi certains objectifs bien spécifiques ont été fixés et comment les directives, les procédures et les mécanismes permettent d'atteindre les objectifs.

Dans la plupart des PME, les objectifs de sécurité ne sont pas fixés. Dans les autres, les gens sont simplement informés qu'une politique a été affichée et qu'elle est disponible. La sensibilisation est parfois présente, du moins lorsque de nouveaux employés sont embauchés. Les connaissances ne sont pas mises à jour régulièrement. La formation est limitée au strict minimum et les rôles clés en matière de sécurité sont peu instruits.

Guidance

Les PME devraient énumérer les connaissances dont leurs employés (et utilisateurs) ont besoin pour

contribuer à la réalisation des objectifs de sécurité de l'information et des activités de l'entreprise. Ceci concerne :

- la politique de sécurité ;
- la politique de confidentialité (en référence aux données à caractère personnel) ;
- les processus et procédures de sécurité à suivre ;
- l'utilisation correcte des informations, des systèmes TIC et des mécanismes de sécurité ;
- les menaces auxquelles ils peuvent être confrontés lors du travail ;
- la réaction à avoir en cas d'anomalies et d'incidents (comme c'est le cas pour l'incendie).

Le contenu doit être fixé, ainsi que le mode de transmission/enseignement le plus approprié.
Un plan et un programme devraient être définis et mis en œuvre pour s'assurer que tout le personnel et certains rôles soient prêts à agir comme attendu.

Après chaque session, et après quelques mois, un test devrait être réalisé pour vérifier les connaissances et les compétences acquises. Cela permet l'adaptation progressive du contenu et du plan au contexte réel, et s'assurer que le personnel applique les règles.

Extension à la vie privée

La sensibilisation à la protection de la vie privée et la formation sont requises par le RGPD, sur une base annuelle.

22 CONTRÔLE #14 : ASPECTS PORTANT SUR LA SÉCURITÉ DE L'INFORMATION DANS LES RELATIONS AVEC LES FOURNISSEURS

Contrôle

Les contrats avec les fournisseurs doivent énoncer clairement les attentes de l'organisation en ce qui concerne la sécurité de l'information, la gestion des incidents, la préparation aux TIC à la continuité des activités.

Objectif

Les PME sont confiantes que leurs fournisseurs savent comment traiter les informations qui leur sont confiées en fonction de leur niveau de classification et de leur rôle et des exigences en cas d'incident et de crise.

Portée

Afin de garantir des accords de confiance avec les fournisseurs et les sous-traitants, ce contrôle concerne :

- les informations de la PME qui sont nécessaires pour exécuter le contrat signé ;
- les attentes et les exigences en matière d'approvisionnement et de prestation des biens et services contractuels ;
- les attentes et exigences à l'appui de la PME en cas d'incident et de crise ;
- les règles à suivre en cas de conflit pendant la durée du contrat ;

- les clauses et règles de fin de contrat (concernant la restitution ou la destruction des informations fournies/stockées).

Afin de s'assurer que l'objectif est atteint, la portée de ce contrôle tient également compte des exigences en matière de sécurité de l'information pendant la phase d'appel d'offres, la préparation, la signature et la maintenance/évolution des attentes contractuelles.

Situation

Chaque partenaire investi dans la relation a ses propres risques. Si un événement se produit des deux côtés, les conséquences pourraient être très différentes. Certains partenaires de la chaîne d'approvisionnement peuvent faire face à des menaces ou à des événements précis qui peuvent compromettre l'ensemble de la chaîne.

Comme le fournisseur doit connaître les risques de l'acquéreur (ou du moins les menaces craintes) pour les contrer, il a accès à des informations clés et leur utilisation abusive est préjudiciable à l'acquéreur.

Le client final (consommateur) a également des risques spécifiques que la chaîne d'approvisionnement devrait identifier et gérer.

Risques liés à l'acquisition de produits (principalement, mais pas seulement, TIC) :

- Pour fournir le « bon » produit, le fournisseur doit connaître les « besoins » de l'acquéreur et certaines informations échangées qui peuvent être sensibles.
- Le défaut de conformité du produit aux spécifications peut avoir une incidence sur la capacité de l'acquéreur à fonctionner, surtout s'il s'agit d'une infrastructure TIC essentielle.
- Les vulnérabilités du produit peuvent compromettre la posture de sécurité de l'acquéreur.
- Accès du fournisseur aux systèmes et aux informations TIC de l'acquéreur.
- L'acquéreur a accès aux systèmes TIC du fournisseur.
- L'acquéreur peut exiger le suivi des processus de production et d'externalisation du fournisseur.

Risques liés à l'acquisition de services

- Accès du fournisseur aux informations de l'acquéreur (externalisation, Cloud, Backups, maintenance des équipements TIC, etc.)
- Le fournisseur a accès aux installations de l'acquéreur (p. ex., services de nettoyage, car les activités se déroulent très souvent en dehors des heures de bureau et les nettoyeurs ont accès à toutes les pièces et à tous les endroits).
- L'acquéreur peut exiger le suivi des processus du fournisseur pour contrôler la qualité (et la sécurité du service, c'est une exigence du RGPD).

Règles relatives au RGPD

- Règles d'accès, d'emplacement de stockage et de conservation des données nominatives de l'acquéreur.
- L'acquéreur doit assurer le contrôle de la chaîne du fournisseur lorsque le fournisseur externalise une partie de ses activités, et veiller à ce que les mêmes

« règles de conformité » soient mises en œuvre.

Écart

Ce contrôle est rarement mis en œuvre par les PME, comme c'est également le cas pour les grandes organisations. C'est probablement dû au fait que l'information n'est pas gérée (voir contrôle #1) et, par conséquent, pas donné une valeur appropriée pour montrer à quel point elle est sensible. Ce contrôle est particulièrement important avec les services cloud.

Guidance

Pour assurer une bonne gestion des risques liés à la sécurité de l'information, une politique devrait énoncer les règles que la PME devrait suivre lorsqu'elle ouvre, signe, exploite et résilie des contrats avec des fournisseurs et des sous-traitants de produits et de services. Cette politique déterminera quel contrôle l'entreprise veut avoir sur la chaîne d'approvisionnement des services/produits du fournisseur.

Au sein des PME, les contrats doivent être préparés et signés par une seule personne de la haute direction. Le contrat doit être fondé sur un objectif clair, car soit l'acquéreur doit soutenir les activités opérationnelles, soit certaines activités particulières dépassent ses compétences, mais sont essentielles pour atteindre les objectifs opérationnels (p. ex., TIC).

Il faut garder à l'esprit le principe de sécurité de l'information du « Privilège minimal » afin que le fournisseur n'ait accès qu'à l'information nécessaire pour « exécuter » le contrat. La protection concerne l'accès et le transfert d'informations sur les trois critères de sécurité : Confidentialité, Intégrité et Disponibilité ! Cela pourrait se faire par :

- La présence et l'activation des bonnes pratiques et processus (ISMS, GDPR, etc.) ;
- Le contrôle de l'accès des fournisseurs aux informations et installations de l'acquéreur ;
- L'entente sur les niveaux de service (SLA) et la fiabilité.

Une liste de contrôle

Le contrat doit contenir des clauses de sécurité et des annexes mutuellement acceptées (par exemple, pour le RGPD ou le produit/service en relation avec les activités critiques de l'entreprise). Ces annexes devraient formuler un ensemble de contrôles et de responsabilités concernant la mise en œuvre et le suivi. Elle contiendront également des règles pour résoudre les conflits dans la mise en œuvre des contrôles et en cas d'incidents liés à la sécurité de l'information, y compris les incidents liés à la vie privée.

- Le contrat devrait définir les protocoles d'échange d'information à utiliser lorsque des « informations protégées » sont partagées.
- Les PME devraient :
    - informer leur personnel des règles fixées par le contrat d'échange d'informations avec les fournisseurs.
    - sensibiliser leur personnel à l'utilisation de services externalisés.
    - informer leur personnel de l'utilisation et de l'entretien du produit acquis.
    - déterminer et surveiller les règles de contrôle d'accès des fournisseurs sur les systèmes TIC de l'entreprise.
    - déterminer et surveiller l'accès physique des fournisseurs/sous-traitants aux installations, comme c'est le cas pour les visiteurs.
- Un registre des produits et services acquis devrait être créé avec la liste des informations concernées et échangées. Ce registre devrait être tenu à jour et examiné pour tout changement dans les contrats ou de niveau de classification de l'information.

Extension à la vie privée

Lorsque le fournisseur a accès aux DCP et doit les traiter, il doit se conformer au RGPD en tant que sous-traitant des données. Toutes ces règles doivent être appliquées lorsque des informations personnelles sont traitées ou échangées avec un fournisseur/sous-traitant, dans l'application du RGPD.

23 CONTRÔLE #15 : ORGANISATION DE LA SÉCURITÉ DE L'INFORMATION

Contrôle

Les rôles essentiels liés à la sécurité de l'information devraient être définis, décrits et attribués à des personnes suffisamment instruites qui devraient relever de la haute direction. L'utilisation d'une matrice RACI est généralement recommandée, car cet outil permet de délimiter clairement toutes les responsabilités et précise quand chaque rôle intervient.

Objectif

Le personnel des PME sait qui est responsable de la sécurité de l'information et des rôles essentiels qui sont activés.

Portée

Ce contrôle porte sur tous les rôles et responsabilités en matière de sécurité de l'information.

Situation

Les rôles en matière de sécurité de l'information sont à peine définis et attribués dans les PME, pour la simple raison qu'il n'y a pas assez de personnel suffisamment formé. Ces rôles sont cependant importants et certains, en particulier ceux liés au RGPD, sont obligatoires.

Guidance

Plusieurs rôles et fonctions sont essentiels pour assurer une gestion cohérente et continue de la sécurité de l'information, tant pour les environnements informatiques que non informatiques. Certains rôles peuvent être attribués à la même personne, à condition que cela ne crée pas de conflit d'intérêts et ne mette pas sur la même personne l'action et son approbation. Tous les rôles devraient rapporter à la haute direction qui prend la décision finale et en assume la responsabilité.

La plupart de ces rôles nécessiteront un « groupe de travail » pour la phase de préparation, car ils ont besoin des connaissances et de la participation de tous les départements. Ces rôles peuvent être externalisés, mais le contrat doit être clair et suivre les recommandations énoncées dans le contrôle no 14. La responsabilité finale incombera toutefois toujours aux PME elles-mêmes.

La structure de l'organisation et du personnel doit être adaptée individuellement aux circonstances de l'entreprise. En ce qui concerne la composition des comités, une distinction doit être faite entre la phase d'introduction et la maintenance du projet.

Au tout début, un chef de projet devrait être désigné pour aborder l'introduction de la sécurité de l'information dans l'entreprise et pour assumer le rôle de Conseiller de sécurité de l'information (CSO).

Il s'agit d'établir, de promouvoir et de coordonner le processus de sécurité de l'information. Pour accomplir ces tâches, il est souhaitable que le CSO dispose de connaissances et d'expérience dans les domaines de la sécurité de l'information et des technologies de l'information. Pour cette raison, le choix de cette personne revient souvent aux employés du service des technologies de l'information. Le rôle du CSO peut être joué en collaboration avec le responsable de la protection des données personnelles ou par un autre employé de l'organisation. Le CSO et ses responsabilités doivent être communiqués à tous les employés. Le CSO rapporte directement à la direction de l'entreprise et est inscrit dans l'organigramme en tant que « poste personnel ».

Nous recommandons de prendre en considération les points suivants lors de la nomination du CSO : Premièrement, dans la mesure du possible, le CSO ne devrait pas être le responsable informatique, car ni l'objectivité ni l'impartialité ne peuvent être maintenues. Deuxièmement, le CSO doit disposer de suffisamment de temps pour accomplir sa tâche. Le temps libre doit tenir compte du fait qu'il faut accorder plus de temps pendant l'introduction du projet que le temps accordé pendant les opérations régulières. Cela devrait être fixé séparément dans la description du rôle. Troisièmement, la formation d'une équipe de sécurité de l'information est un élément essentiel de l'établissement, de la mise en œuvre et du maintien d'un processus de sécurité de l'information.

Les personnes ou les responsables suivants doivent être nommés à l'équipe de sécurité de l'information de base, et tous doivent relever de la haute direction pour les décisions et les ressources nécessaires :

Gestionnaire des risques

Ce rôle doit tenir compte de tous les risques auxquels la PME pourrait être confrontée (physiques, juridiques, contractuels, informationnels, informatiques, etc.). Le gestionnaire des risques est responsable de ce qui suit :

- recueillir des renseignements sur les menaces et les vulnérabilités qui y sont liées ;
- calculer le niveau de risque en fonction de la vraisemblance qu'un événement se produise et de la gravité de l'impact opérationnel et des conséquences pour l'entreprise en cas d'occurrence ;
- analyser les solutions et contrôles potentiels pour faire face à ces risques ;
- tenir la haute direction au courant de la situation et recevoir d'elle la décision et les ressources nécessaires.

Responsable sécurité de l'information (RSI)

Ce rôle concerne tous les types de supports d'information et leur gestion. Le gestionnaire de la sécurité de l'information est responsable de ce qui suit :

- assurer la coordination avec le gestionnaire des risques en ce qui concerne les risques pour l'information – il peut, s'il est suffisamment formé, assurer la gestion des risques liés à la sécurité de l'information au nom du gestionnaire des risques ;

- préparer, coordonner et surveiller le plan d'action en matière de sécurité de l'information qui a été décidé par la haute direction ;
- préparer, coordonner et surveiller le programme de sensibilisation et de formation.

Responsable des incidents

Ce rôle concerne tous les types d'incidents et notamment ceux liés à l'information dans l'application du contrôle #4. Le gestionnaire des incidents travaille en étroite collaboration avec le gestionnaire de la sécurité de l'information et est responsable de ce qui suit :

- établir la liste des événements que la PME veut contrôler ;
- préparer et proposer :
  - les critères visant à promouvoir un événement lié à la sécurité de l'information au niveau d'incident ;
  - un ensemble de mesures et de ressources pour contrôler l'incident ;
  - les procédures et les mécanismes permettant de signaler l'événement au point de contact ;
- proposant :
  - la structure et les compétences requises de l'équipe d'intervention en cas d'incident (IRT). Il est à noter que plusieurs IRT peuvent exister selon le type d'incident, sa source et ses conséquences ;
  - la création d'un rôle de « gestionnaire des incidents » qui coordonne les activités des IRT ;
  - un processus visant à tirer des leçons des incidents visant à réduire les incidents futurs et/ou à améliorer l'intervention.
  - les critères pour déclarer l'incident clos ;
  - conserver tous les événements et incidents dans un registre ou une base de données.

Responsable vulnérabilités

Ce rôle concerne les vulnérabilités des TIC et en particulier celles qui s'appliquent aux composantes TIC critiques. Le gestionnaire des vulnérabilités travaille en étroite collaboration avec le gestionnaire des risques, le gestionnaire de l'information et le gestionnaire des incidents. Il est responsable:

- d'identifier les vulnérabilités et les communiquer au gestionnaire des risques ;
- de préparer et proposer des solutions pour éliminer les vulnérabilités ;
- d'aider le gestionnaire d'incident à élaborer la réponse à l'incident causé par les vulnérabilités ou introduit par celles-ci.

Gestionnaire de problèmes

Ce rôle concerne tous les événements, situations et conditions qui ne touchent pas immédiatement les objectifs de sécurité de l'information, mais qui peuvent les compromettre s'ils sont combinés. Il s'attaque à la partie non ICT des vulnérabilités auxquelles les PME pourraient faire face et ses responsabilités sont très proches du gestionnaire de vulnérabilité. Le gestionnaire de problèmes doit :

- identifier ces événements et conditions de survenance ;
- élaborer des solutions de rechange pour permettre la préservation des

opérations commerciales tout en « réparant » la situation.

Responsable crise

Ce rôle concerne les situations qui touchent sérieusement la capacité opérationnelle lorsqu'un rôle clé est absent de façon inattendue pour prendre une décision ou agir comme prédéfini, ou lorsqu'un processus clé (ou composant technologique clé permettant son fonctionnement) est défectueux. La coordination étroite avec le responsable de l'incident et le responsable des risques est obligatoire, car, ici, la conséquence potentielle est la fin de l'activité. Ce rôle consiste à :

- déterminer les situations et les conditions qui peuvent nuire aux objectifs d'entreprise ;
- évaluer la durée de l'interruption du service ou de l'exploitation — ou de la perte de données — qui est considérée comme « à la limite » de l'atteinte des objectifs d'entreprise ;
- analyser et proposer des solutions de rechange, des procédures et les ressources nécessaires pour renforcer la résilience métier et technologique.

Responsable conformité

Ce rôle concerne tous les aspects commerciaux et opérationnels régis par des règlements ou des exigences contractuelles. Ce rôle devrait être attribué à un membre du conseil de direction. Le responsable de la conformité est chargé :

- d'identifier les lois et les exigences contractuelles ;
- d'identifier les défauts de conformité et proposer des solutions ;
- de communiquer régulièrement avec les autres rôles pour promouvoir la conformité.

Extension à la vie privée

Délégué à la protection des données (DPO) :
Le DPO est un responsable conformité dans l'application du RGPD. Ce rôle est obligatoire dès que les DCP sont traitées par la PME. Le DPO devrait être indépendant de tout rôle ou comité décisionnel au sein de la PME.

24 CONTRÔLE #16 CONTRÔLES SUPPLÉMENTAIRES DE PROTECTION DE LA VIE PRIVÉE

Contrôle

Voici quelques contrôles de confidentialité spécifiques qui peuvent être pertinents pour les besoins du traitement des données personnelles d'une PME.

Ce contrôle est basé sur la norme ISO/IEC 27701 « Extension aux normes ISO/IEC 27 001 et ISO/IEC 27 002 pour la gestion des informations relatives à la vie privée — Exigences et lignes directrices » et complète les contrôles de sécurité généraux décrits dans les contrôles précédents et les spécialisations pertinentes en matière de vie privée, lorsque présents. L'objectif est de fournir un outil qui permet à la PME d'effectuer une évaluation initiale pour identifier les problèmes potentiels de conformité au RGPD. La résolution de ces problèmes nécessite un soutien spécialisé.

Objectif

En général, les exigences de la norme ISO/CEI 27001:2013 relatives à la « sécurité de l'information » sont étendues à la protection de la vie privée susceptible d'être affectée par le traitement des données à caractère personnel. Le cas d'une PME agissant en tant que sous-traitant traitant des données à caractère personnel pour le compte du responsable du traitement n'est pas pris en compte. En effet, les principes sont les mêmes, mais il s'agit généralement d'un contexte dans lequel le traitement des données à caractère personnel est le cœur de métier d'une PME. Cette question est trop complexe pour être couverte de manière significative par un guide simplifié et est susceptible de nécessiter une analyse approfondie.

Portée

Cet ensemble de contrôles concerne le traitement des DCP pour une PME agissant en tant que responsable du traitement. Cela couvre les cas où il est nécessaire de déterminer les finalités et les moyens du traitement des données à caractère personnel.

Situation

L'objectif des contrôles vie privée décrits dans cette section est de permettre de traiter les questions suivantes :

- **les conditions de collecte et de traitement des données à caractère personnel** : les PME devraient déterminer et documenter que le traitement des

données à caractère personnel est légal et possède une base juridique conformément au RGPD ou à une législation spécifique, avec des objectifs clairement définis et légitimes ;

- **les obligations à l'égard des personnes concernées :** les PME devraient veiller à ce que des informations appropriées soient fournies aux personnes concernées au sujet du traitement de leurs données à caractère personnel et à ce que toutes les autres obligations applicables aux personnes concernées en matière de traitement des DP soient respectées ;
- **la protection de la vie privée par défaut et dès la conception** : les PME devraient veiller à ce que les processus et les systèmes soient conçus de manière à ce que la collecte et le traitement des données personnelles (y compris l'utilisation, la divulgation, la conservation, la transmission et l'élimination) soient limités à ce qui est nécessaire aux fins déterminées ;
- **le partage, le transfert et la divulgation de données personnelles :** les PME devraient déterminer et documenter lorsque des données personnelles sont transférées à d'autres juridictions ou à des tiers et/ou divulguées conformément aux obligations applicables.

Guidance

A. Conditions de collecte et de traitement des données à caractère personnel

Cet ensemble de contrôles couvre les conditions de collecte et de traitement des données à caractère personnel :

- identifier et documenter les finalités spécifiques pour lesquelles les données à caractère personnel sont traitées ;
- déterminer, documenter et respecter le RGPD et toute législation applicable (par exemple la directive ePrivacy ou les futures réglementations) aux finalités identifiées ;
- obtenir et enregistrer le consentement des personnes concernées selon des processus documentés permettant de démontrer si, quand et comment le consentement a été obtenu ;
- évaluer la nécessité d'une évaluation des impacts sur la vie privée et, le cas échéant, la mettre en œuvre chaque fois qu'un nouveau traitement ou une modification du traitement existant est prévu ;
- veiller à ce que des contrats écrits soient conclus avec tout processeur de données à caractère personnel utilisé, en veillant à ce qu'ils adressent la mise en œuvre des contrôles appropriés ;
- déterminer les rôles et responsabilités respectifs pour le traitement des données à caractère personnel en cas de traitement conjoint de ces données ;
- déterminer et conserver en toute sécurité les dossiers nécessaires à l'appui de ses obligations en matière de traitement des données à caractère personnel.

B. Obligations envers les personnes concernées

Cet ensemble de contrôles couvre les obligations envers les personnes concernées :

- déterminer et documenter les obligations légales, réglementaires et commerciales envers les personnes concernées liées au traitement de leurs

données personnelles et fournir les moyens de remplir ces obligations ;

- déterminer et documenter les informations à fournir aux personnes concernées concernant le traitement de leurs données à caractère personnel et le calendrier d'une telle disposition ;
- fournir aux personnes concernées des informations claires et facilement accessibles identifiant le responsable du traitement et décrivant le traitement de leurs données à caractère personnel ;
- fournir un mécanisme permettant aux personnes concernées de modifier ou de retirer leur consentement et de s'opposer au traitement de leurs données à caractère personnel ;
- mettre en œuvre des politiques, des procédures et/ou des mécanismes pour respecter leurs obligations envers les personnes concernées d'accéder, de corriger et/ou d'effacer leurs données ;
- informer les tiers avec lesquels les données à caractère personnel ont été partagées de toute modification, retrait ou objection concernant les données à caractère personnel partagées, et mettre en œuvre les politiques, procédures et/ou mécanismes appropriés à cette fin ;
- être en mesure de fournir une copie des données à caractère personnel traitées à la demande de la personne concernée ;
- définir et documenter les politiques et procédures de traitement et de réponse aux demandes légitimes des personnes concernées ;
- identifier et traiter les obligations (légales) envers les personnes concernées résultant de décisions relatives à la personne concernée fondées sur le traitement automatisé des données à caractère personnel.

C. Protection de la vie privée par défaut

Cet ensemble de contrôles couvre la « protection des DCP dès la conception » et également « par défaut » :

- limiter la collecte de données à caractère personnel au minimum pertinent, proportionnel et nécessaire aux finalités identifiées ;
- limiter le traitement des données à caractère personnel à celui qui est adéquat, pertinent et nécessaire aux finalités identifiées ;
- s'assurer et documenter que les données à caractère personnel sont aussi exactes, complètes et à jour que nécessaire aux finalités pour lesquelles elles sont traitées, tout au long du cycle de vie de ces données ;
- définir et documenter les objectifs de minimisation des données et les mécanismes (comme la pseudonymisation[17]) utilisés pour atteindre ces objectifs ;
- soit supprimer les données à caractère personnel, ou les mettre sous une forme qui ne permet plus l'identification ou la réidentification des personnes concernées, dès que les données originales ne sont plus nécessaires aux fins identifiées ;
- avoir des politiques, des procédures et/ou des mécanismes documentés pour l'élimination (p. ex., effacement ou destruction) des données personnelles et veiller à ce que les fichiers temporaires créés à la suite de leur traitement soient éliminés selon des procédures documentées dans un délai précis et documenté ;

[17] Tel que défini par le RGPD : remplacer toute information qui pourrait être utilisée pour identifier une personne avec un pseudonyme, ou, en d'autres termes, une valeur qui ne permet pas d'identifier directement la personne.

- ne conservent pas les données à caractère personnel pendant une période plus longue que la période nécessaire à leur traitement ;
- soumettre les données à caractère personnel transmises sur un réseau de transmission de données à des contrôles appropriés visant à garantir qu'elles atteignent leur destination prévue.

D. Partage, transfert et divulgation de données personnelles

Cet ensemble de contrôles couvre le partage, le transfert et la divulgation des données personnelles :

- identifier et documenter la base pertinente pour les transferts de données à caractère personnel entre juridictions ;
- préciser et documenter les pays et les organisations internationales auxquels les données à caractère personnel peuvent éventuellement être transférées ;
- enregistrer les transferts de données à caractère personnel à destination ou en provenance de tiers et assurer la coopération avec ces parties pour soutenir les demandes futures liées aux obligations envers les personnes concernées ;
- consigner les divulgations de données personnelles à des tiers, y compris les données personnelles qui ont été divulguées, à qui et à quel moment.

25 CONCLUSION

Utiliser les technologies permettant l'innovation, la production, et la fourniture de solutions devient de plus en plus partie intégrante de chaque processus d'affaires des PME. Cela correspond naturellement à l'objectif à long terme de la transformation numérique, y compris un niveau de base d'intensité numérique pour la plupart des PME européennes comme communiqué dans le DIGITAL DECADE. Toutefois, la cybersécurité demeure une préoccupation majeure pour les PME et l'une des principales menaces à la continuité et à la survie des activités !

Comme les menaces à la sécurité sont récurrentes, un processus de sécurité de l'information est nécessaire pour protéger trois valeurs fondamentales : la confidentialité, l'intégrité et la disponibilité de l'information. Par conséquent, les technologies de l'information et la cybersécurité sont devenues un préalable fondamental au développement personnel des individus et de l'économie dans l'Union européenne ainsi que dans le monde. Certaines conditions préalables sont nécessaires pour établir la sécurité de l'information dans une entreprise afin d'assurer et de maintenir le niveau de conformité requis.

La protection de l'information est un élément crucial des politiques, des lignes directrices, des recommandations et des standards en matière de cybersécurité pour assurer la conformité. L'ISO/CEI 27002 est l'une des nombreuses ressources traitant de la protection des données. Toutefois, il s'agit d'un document complexe que de nombreuses PME trouveraient difficile et coûteux à mettre en œuvre. Ce guide aide les PME à mettre en œuvre les contrôles minimaux recommandés pour protéger leurs informations, maintenir la confiance des consommateurs et se conformer aux règles du RGPD. La section 7 demeure en grande partie une section technique que les professionnels des TIC et de la cybersécurité dans les PME — les facilitateurs numériques — utiliseraient pour les aider à mettre en œuvre les contrôles recommandés pour réduire le risque d'attaques sur la cybersécurité.

La cible principale de ce guide est les PME (non-TIC) qui doivent comprendre l'importance de protéger l'information et de se conformer à différentes lois, y compris le RGPD. Par conséquent, ce guide vise à sensibiliser les PME et à guider leur direction à travers une stratégie et une politique efficace de protection des données. Les PME et les professionnels des TIC peuvent consulter la section 7 pour obtenir de plus amples conseils techniques sur la mise en œuvre des 16 contrôles de sécurité et les utiliser pour aider et conseiller les PME sur les mesures les plus appropriées.

Ce guide a montré comment les normes aideraient les PME à protéger leurs renseignements de façon rapide et rentable. Il a également souligné la nécessité pour les PME d'être au courant de la conformité au RGPD puisqu'elles traitent des renseignements personnels dans de nombreuses situations. À cet égard, il s'est concentré sur la protection de la vie privée en tant que pilier important du RGPD, où le traitement et la libre circulation des données à caractère personnel sont équilibrés avec la protection des droits et libertés fondamentaux des personnes, notamment leur droit à la protection leurs données personnelles, c'est-à-dire protéger leur vie privée.

Le guide soutient également que la mise en œuvre efficace des contrôles de sécurité n'est pas possible sans une stratégie de sécurité solide et des objectifs de sécurité clairs. Alors que les normes (et les contrôles — ISO/CEI 27 014 dans ce cas — se concentrent sur ce qu'une entreprise doit mettre en œuvre, il y a peu de conseils sur la façon de les mettre en œuvre. Par conséquent, des connaissances spécialisées sont nécessaires pour porter la stratégie définie par la direction aux processus et procédures concrets et mesurables à travers le COBIT.

Enfin, le guide a introduit 16 contrôles de sécurité comme contrôles minimaux recommandés, que les PME doivent mettre en œuvre afin de protéger leurs informations et de se conformer aux règles du RGPD. Ces contrôles abordent les questions personnelles, organisationnelles et techniques afin d'assurer une protection complète liée, entre autres, à :

1. Gérer et protéger les actifs numériques
2. Réagir aux cyberattaques
3. Établir des politiques de partage de données, de sauvegarde et de télétravail
4. Assurer des mesures de protection pour minimiser les vulnérabilités et les cybermenaces et maintenir la continuité des activités après une cyberattaque

1 ANNEXE A : TECHNIQUE DE CLASSIFICATION DE L'INFORMATION

1.1 Introduction

Comme mentionné dans l'introduction du présent guide, nous savons que l'information a divers buts ou objectifs. Les processus opérationnels sont là pour atteindre ces objectifs et, parfois, ce sont les informations d'entrée qui sont les plus importantes, parfois ce sont les sorties, parfois les deux.

La valeur de l'information devrait être définie en fonction des objectifs opérationnels ou des conséquences si ces objectifs ne sont pas atteints.

Quatre axes de mesure de la valeur ont été identifiés :

- **Valeur propre** : ce qu'il en coûte pour acquérir et conserver l'information ; par exemple, ce qui est directement disponible sur Internet est gratuit et ne nécessite aucun entretien ; une base de données avec ses métadonnées qui doit rester à jour est une autre histoire ;
- **Valeur d'utilisation :** la quantité et l'importance de ce que nous pouvons faire si l'information correspond à nos besoins ; cela est directement lié aux objectifs métiers ; par exemple, une voiture nous permet de voyager pour rencontrer des clients ou de partir en vacances ;
- **Valeur de perte :** ce que nous ne pouvons plus faire si la qualité de l'information est dégradée ou si les critères de sécurité ne sont plus respectés ; par exemple, un pneu crevé ou un manque de carburant nous bloque dans notre déplacement et nous pouvons rater une opportunité ou un contrat, ou bien nous manquons notre avion avec des conséquences financières… la voiture est cependant toujours là et peut être réparée ;
- **Valeur d'attraction :** l'information dont nous avons besoin pourrait être très intéressante pour les « autres » afin de nous empêcher d'atteindre nos objectifs… ou de les atteindre avant nous.

Ces quatre axes n'ont pas le même poids par rapport aux critères de sécurité (confidentialité, intégrité, disponibilité).
La valeur de l'information devrait être évaluée pour chaque critère de sécurité.

1.2 Procédure

À faire en équipe avec la direction

1. Énumérer les enjeux de l'entreprise par ordre décroissant d'importance (voir tableau 1).
2. Établir des échelles qualitatives de gravité des conséquences au cas où les enjeux et les valeurs seraient endommagés (quatre niveaux devraient suffire – un nombre pair empêche l'utilisation simpliste d'une position moyenne choisie lorsque nous ne savons pas, voir le tableau 2).
3. Créer des catégories d'information de même nature (financière, opérationnelle, liée aux personnes…) ou liées au même processus/activité d'affaires, et choisir une information représentative pour chaque catégorie.
4. Énumérez les DIX processus opérationnels les plus importants pour l'entreprise (classés par ordre décroissant) afin d'atteindre ses objectifs, avec les trois à cinq informations clés (en entrée ou en sortie).
5. Identifier trois à cinq composantes TIC clés qui permettent d'atteindre les objectifs des processus énumérés.

Reproduire cette procédure au moins une fois par an, peut-être avec différents processus et informations pour s'assurer que toutes les catégories d'informations clés ont été classifiées. Par cette procédure, nous identifions et classifions (évaluer la valeur) les catégories d'informations à protéger. Une fois les informations clés classifiées, toutes celles de sa catégorie recevront la même valeur et, par conséquent, le même niveau de protection.

Certaines catégories clés pourraient être associées à des processus opérationnels clés ; ils devraient toutefois être protégés de manière adéquate. Ici, ce qui compte, c'est la catégorie d'information et non le processus clé.

Remarque : Le processus métier reçoit le niveau de classification de l'information la plus précieuse. Les composantes des TIC héritent du niveau de classification du processus qu'elles soutiennent ou de l'information qu'elles contiennent. Cela est essentiel pour déterminer leur importance métier pour le plan de continuité des activités (PCA/BCP) et la gestion des incidents.

À faire par le « propriétaire » du processus métier

Pour chaque processus ou information choisi :

- Déterminez les enjeux qui seront touchés si le résultat du processus ou de l'activité n'atteint pas les attentes (pour l'entreprise ou le client). Chaque processus d'information aboutira probablement à des enjeux différents.
- Pour chaque information choisie, déterminez à l'aide du tableau 2 le besoin de protection/sécurité en termes de confidentialité, d'intégrité et de disponibilité. Le besoin de sécurité sera hérité par toutes les informations de la catégorie représentée, qu'elles soient déjà utilisées ou nouvelles (acquises ou produites).
- Protégez l'information selon le besoin de sécurité.

Cette procédure doit être répétée au moins une fois par an, car beaucoup de choses peuvent changer dans le contexte de l'entreprise ou de ses objectifs.

A. Enjeux

Les enjeux sont, comme au poker ou dans un pari, ce que nous mettons sur la table et que nous ne voulons pas perdre. Il existe **neuf** types d'enjeux, chacun pouvant contenir différents niveaux :

Enjeu	Niveau
Réputation	• Perte de confiance interne • Perte d'image externe ou de crédibilité • Perte de réputation technologique (compétences, aptitudes) • Perte d'avantage concurrentiel • Perte de leadership technologique • Perte de capacité de négociation
Conséquences juridiques ou judiciaires	• Non-conformité juridique • Incapacité de satisfaire aux obligations légales • Effet négatif sur le respect général de la loi • Conflit judiciaire • Poursuites judiciaires et/ou amendes
Atteinte à la vie privée	• Réduction de la capacité des personnes à poursuivre une vie personnelle, familiale, sociale, judiciaire et économique normale • Difficulté à trouver un emploi
Perte financière (directe ou indirecte)	• Pertes financières (en conséquence de l'événement) • Coûts d'urgence et de réparation (RH, équipement, études, évaluation, etc.) • Perte de parts de marché • Perte de biens ou d'actifs • Perte de clients
Problèmes sociaux ou industriels	• Crise sociale – Grève • Démission forcée • Licenciement • Fermeture d'entreprise • Chômage de longue durée
Impact opérationnel	• Interruption de service (à la suite de l'événement : p. ex., tant que le problème n'est pas résolu) • Perte d'efficacité interne, perturbations/interruptions opérationnelles internes • Difficultés organisationnelles internes (réorganisation, perte de ressources humaines, etc.) • Perte de fournisseurs

Problèmes contractuels (avec les clients ou les fournisseurs)	• Perturbations/interruptions opérationnelles de tiers • Difficultés contractuelles • Incapacité à respecter les clauses contractuelles
Mise en danger physique de personnes (santé, blessures, décès)	• Affaiblissement de la capacité de protéger adéquatement les personnes • Danger pour l'environnement (pollution) - affaiblissement de la capacité de préserver l'environnement et de lutter contre la pollution
Atteinte à la confidentialité des informations confiées (classifiées ou détenues par des tiers)	

Tableau 1 : Enjeux

Vous devrez sélectionner plusieurs impacts pour évaluer la valeur de l'information :

- au moins TROIS (3) pour acquérir une vue non linéaire de la situation et avoir une vision générale moins sensible à l'évidence (qui est souvent trompeuse) et plus stable le long du temps ;
- maximum de CINQ (5) pour que l'évaluation soit gérable dans le temps.

B. Besoin de sécurité

Dans le tableau 2, chaque critère de sécurité est divisé en plusieurs questions :

- Confidentialité : lorsque le processus l'exige, il est important de séparer les données d'entrée et de sortie. Selon la catégorie d'information et la taille des entreprises, il serait essentiel de séparer les atteintes à la confidentialité aux personnes internes (qui ne participent pas au processus) et au monde extérieur.
- Intégrité : nous devrions rechercher le besoin lié à l'information d'entrée et de sortie, qui tient également compte du problème d'intégrité du processus (automatisé).
- Disponibilité : il est essentiel de séparer les conséquences (et le besoin de protection) en raison de problèmes de courte durée (perturbations) de ceux liés à des événements à long terme (y compris la destruction). Le tableau 3 permet de délimiter clairement les deux durées.

0	Aucun effet
1	Effet sensible, mais sans conséquence ; faible impact
2	Effet acceptable et gérable ; impact modéré
3	Effet difficilement acceptable et gérable ; impact élevé
4	Effet catastrophique impossible à gérer ; impact exceptionnel

Tableau 2 : Niveau d'impact sur les enjeux

Critère/dommages	**Enjeu 1**	**Enjeu 2**	**Enjeu 3**	**Enjeu 4**	**Enjeu 5**	**Besoin de sécurité**

Confidentialité	**0**	**0**	**0**	**0**	**0**	**0**
Compromission interne de l'information d'entrée						0
Compromission interne de l'information de sortie						0
Compromission externe de l'information d'entrée						0
Compromission externe de l'information de sortie						0
Intégrité	**0**	**0**	**0**	**0**	**0**	**0**
Donnée de sortie erronée						0
Donnée d'entrée erronée						0
Disponibilité	**0**	**0**	**0**	**0**	**0**	**0**
Indisponibilité acceptable						0
Indisponibilité inacceptable						0
TOTAL (critère)	**0**	**0**	**0**	**0**	**0**	**0**

Tableau 3 : Classification des informations

Remarque : sur chaque ligne du tableau 3, comme pour chaque critère (deux lignes), le « besoin de sécurité » est la valeur maximale obtenue. C'est en effet le besoin le plus important dont il faut tenir compte.
Vous découvrirez facilement que les enjeux et les valeurs obtenues peuvent être différents pour chaque (catégorie d') information et processus reliés. Il s'agit d'un objectif à atteindre et restera indépendant des contrôles de sécurité sélectionnés mis en œuvre pour couvrir les risques.

Durée d'indisponibilité (pour l'information ou la technologie)	**Niveau de préjudice**	**AAF**	**AUD**	**MAU**
≤ 5 minutes				
≤ 30 minutes				
≤1 heure				
≤ ½ journée				
≤ 1 jour				
≤ ½ semaine				
≤ 1 semaine				
≤ ½ mois				
≤ 1 mois				

Tableau 4 : Détermination du seuil entre indisponibilité courte et longue

AAF : Fréquence annuelle acceptable

AUD : Annual Unavailability Duration : Durée d'indisponibilité x AAF.
MAU : Valeur moyenne de l'indisponibilité annuelle (AUD) – la somme des différents AUD/9. Tout ce qui est en dessous de ce seuil est acceptable dans le tableau 2, ce qui est au-dessus, est inacceptable.

C. Protection des informations

Le niveau de protection peut être défini en termes généraux :

0	Non
1	Élémentaire
2	Bonnes pratiques
3	Meilleures pratiques
4	État de l'art

Les niveaux 4 et 3 devraient d'abord être assurés. Les autres besoins seront naturellement couverts par les contrôles pris, au moins dans les premiers mois. D'autres contrôles peuvent être ajoutés si la surveillance en montre le besoin.

Remarque : en plus de leur importance opérationnelle pour atteindre les objectifs, les processus héritent de la valeur (et de la protection) de l'information qu'ils traitent ou créent.
Les actifs TIC héritent du niveau de classification des processus et des informations qu'ils contiennent.
Pour chaque critère, le niveau de protection possède également une signification plus précise et pratique.
Chaque niveau de protection s'appuie sur le précédent.

Confidentialité

1	Accessible à tout le personnel de l'entreprise/de l'organisation ou selon le besoin de connaissance. Ne doit pas quitter les locaux et les systèmes de l'entreprise/organisation sans besoin explicite de connaissance (besoin de partage). Des accords de non-divulgation appropriés doivent être mis en place.
2	Seul le personnel autorisé peut y avoir accès en cas de besoin. La liste de distribution doit être maîtrisée. Cela s'applique par exemple aux informations nécessaires aux opérations quotidiennes, mais protégées par la loi, telles que les enregistrements de données.

3	Contrôle d'accès discrétionnaire (DAC). L'information ne peut quitter les locaux de l'entreprise/de l'organisation sans l'approbation du propriétaire des actifs et un contrôle approprié (cryptage ou contrôle d'accès physique). Stockage dans des environnements contrôlés. Chiffrement recommandé. Stockées au repos dans des armoires verrouillées au moins lorsqu'elles sont imprimées, dans des bases de données et des systèmes de fichiers. L'isolement des éléments n'est pas obligatoire (les informations confidentielles peuvent être stockées dans la même instance d'une base de données que les informations non confidentielles tant que le niveau approprié de contrôle d'accès est en place). Les données peuvent être stockées dans le Cloud à condition que : 1) le fournisseur de services Cloud ait été approuvé avec succès du point de vue de la sécurité et de la gestion des risques ; 2) au moins le même niveau d'identification de l'utilisateur, d'identité et de gestion des accès est en place (par rapport à l'entreprise/organisation interne).
4	L'accès aux données est strictement contrôlé, c'est-à-dire via un Contrôle d'accès obligatoire (MAC). Chaque élément est isolé des autres dans un conteneur individuel très solide : différentes instances de bases de données (avec cryptage) pour différents types d'ensembles de données. Les données doivent être stockées dans un coffre-fort. Chiffrement requis. Les informations ne peuvent pas être sorties des bureaux sans un contenant physique très solide. La transmission des données physiques aux individus doit être enregistrée. Les informations physiques doivent être individualisées dans la mesure du possible (numéros uniques, copies aux personnes inscrites, etc.) Par défaut, les données hautement confidentielles ne doivent pas être stockées ou traitées dans le Cloud, sauf si des mécanismes d'authentification et de chiffrement appropriés sont en place. Ces mécanismes (et l'architecture de mise en œuvre proposée) devront toujours être examinés et approuvés par le management de la sécurité.

Intégrité

1	Aucun
2	Gérée : L'intégrité est vérifiée par l'utilisateur à la source ou à la fin du processus ; l'information est corrigée lorsque l'écart est constaté, selon les directives et dans les délais définis par le propriétaire. Les sauvegardes sont un moyen de récupérer les informations correctes.
3	Contrôlée : Prévention des problèmes d'intégrité sur l'ensemble du processus ; Détection a posteriori (dans un court délai à définir par le propriétaire) ; les problèmes doivent être signalés au propriétaire de l'actif. Ce contrôle est fourni par exemple par défaut par les systèmes de base de données et par les systèmes de stockage sécurisés. Documents en lecture seule, sauf pour le personnel autorisé.

4	Inaltérable : Les problèmes d'intégrité sont évités. Contrôles d'intégrité obligatoires sur les documents et bases de données (hash/Checksum) ; les documents sont stockés dans un format inaltérable. Détection en temps réel. Les problèmes sont immédiatement signalés au propriétaire qui contrôle la correction.

Disponibilité

1	Aucune RTO : 7 jours ; RPO : 3 à 7 jours
2	Un remplacement est prévu ; le remplacement est planifié et se fait selon les conditions définies par le propriétaire ou l'autorité responsable. RTO : <= 48 h ; RPO : <= 24 heures
3	Une maintenance proactive est recommandée. L'état est surveillé. L'indisponibilité est planifiée et le remplacement réalisé dans un court délai défini par l'autorité responsable. RTO : < 24 h ; RPO : < 8 h
4	L'indisponibilité est évitée et le remplacement est immédiat ; les systèmes sont entièrement redondants, et les données sont reproduites en (quasi) temps réel (miroirs ou techniques d'expédition de journaux). La maintenance proactive est obligatoire sur les systèmes et les applications. Le système est continuellement géré et surveillé. Des contrats de support système et applicatif très importants sont en place (or, platine ou sur mesure). RTO : < 4 h ; 0<= RPO <= 15 minutes, selon la technologie disponible.

° RTO (Recovery Time Objective) : désigne le temps maximum accordé pour reprendre une activité, récupérer des ressources ou fournir des produits ou des services après un incident perturbateur. Cette période cible doit être suffisamment courte pour que les effets négatifs ne deviennent pas inacceptables.
° RPO (Recovery Point Objective) : Point dans le passé où l'information ou son traitement doit être rétabli après un incident perturbateur afin de permettre à une activité de reprendre après un incident perturbateur. En d'autres termes : combien d'informations peuvent être perdues (à partir des dernières modifications ou mises à jour) sans causer trop de problèmes.
Le RPO est utilisé pour garantir que le RTO est réalisable, mais aussi pour documenter la quantité d'information ou de traitement qui peut être perdue en cas de perturbation.

Le contrôle de l'accès à l'information suit également le besoin évalué de protection.

Contrôle d'accès

1	Accessible au personnel de l'entreprise/de l'organisation ; contrôle d'accès standard applicable. Authentification à un facteur.
2	Accès contrôlé basé sur les rôles (RBAC) ; seul le personnel autorisé a accès, et celui-ci est enregistré = uniquement pour les informations à diffusion restreinte.
3	Contrôle d'accès discrétionnaire (DAC) ; le personnel autorisé peut accéder au besoin, la transmission (si justifiée) est autorisée sous la permission du propriétaire. Authentification à deux facteurs.

4	Contrôle d'accès obligatoire (MAC) ; accès individuel ; la demande de transmission doit être justifiée et est faite par le propriétaire. Authentification multifactorielle (2 ou plus).

RBAC (Role-based access control) est un mode par lequel les utilisateurs reçoivent un profil fonctionnel dont les règles sont définies dans les systèmes.

Le DAC (Contrôle d'accès discrétionnaire) est un mode par lequel le propriétaire d'actifs détermine les règles d'accès pour les personnes identifiées et dont le contrôle est délégué au gestionnaire des actifs.
MAC (Contrôle d'accès obligatoire) est un mode par lequel le propriétaire de l'actif non seulement définit mais gère les règles d'accès (pas de délégation).

Il y a trois types de facteurs d'authentification : quelque chose que vous savez (par exemple, un mot de passe), quelque chose que vous possédez (par exemple, un jeton ou une clé) et quelque chose que vous êtes (p. ex. biométrique). L'authentification à trois facteurs (combinaison des trois types) est utilisée exceptionnellement et rarement observée dans les entreprises commerciales.

2 ANNEXE B : LISTE DES TITRES DE CONTRÔLE AVEC LEUR NUMERO, PAR REFERENCE

La référence principale est l'ISO/IEC JTC1 SC27 27002:2013 « Code of practice for information security controls ».

La nouvelle version de la norme ISO/CEI 27002:2022 contient différents numéros de section. Si vous utilisez la version la plus récente, vous pouvez consulter les numéros de section correspondants sur cette page.

Section du présent guide	**Référence ISO**
5. Protection de la vie privée	ISO/CEI 27701
6. Gouvernance de la sécurité de l'information	ISO/CEI 27014
Contrôle #1 Gestion des biens	ISO/CEI 27002 8.1.1 Inventaire des actifs 8.1.2 Propriété des actifs 8.2.1 Classification des informations 8.2.2 Étiquetage des informations 8.2.3 Traitement des actifs 8.3.2 Gestion des biens amovibles Élimination des supports 8.3.3 Transfert de support physique
Contrôle #2 Politiques, normes et lignes directrices	ISO/CEI 27002 5.1.1 Politiques de sécurité de l'information 5.1.2 Révision des politiques de sécurité de l'information
Contrôle #3 Gestion des incidents	ISO/CEI 27002 16.1.1 Responsabilités et procédures 16.1.2 Signalement des événements liés à la sécurité de l'information 16.1.4 Évaluation et décision sur les événements liés à la sécurité de l'information 16.1.5 Réponse aux incidents de sécurité de l'information 16.1.6 Apprendre des incidents de sécurité de l'information ISO/CEI 27035-1 « Gestion des incidents de sécurité de l'information – Partie 1 Principes et processus »
Contrôle #4 Gestion du contrôle d'accès	ISO/CEI 27002 9.1.1 Politique de contrôle d'accès 9.2.1 Enregistrement et désinscription des utilisateurs 9.2.2 Fourniture d'accès utilisateur 9.2.3 Gestion des accès privilégiés 9.2.4 Gestion des informations d'authentification secrètes des utilisateurs 9.2.5 Révision des droits d'accès

Contrôle #5 Sécurité des réseaux et échanges de données	ISO/CEI 27002 13.1.1 Contrôles réseau 13.1.3 Ségrégation dans les réseaux 13.2.1 Politiques et procédures de transfert d'information 13.2.2 Accords de transfert d'informations 13.1.4 Accords de confidentialité ou de non-divulgation ISO/CEI 27 010 « Gestion de la sécurité de l'information pour les communications intersectorielles et inter-organisations »

Section du présent guide	**Référence ISO**
Contrôle #6 Gestion des vulnérabilités	ISO/CEI 27002 12.6.1 Gestion des vulnérabilités techniques 12.6.2 Restriction de l'installation des logiciels 16.1.3 Signalement des faiblesses en matière de sécurité de l'information
Contrôle #7 Lutte contre les logiciels malveillants	ISO/CEI 27002 12.2.1 Contrôles contre les logiciels malveillants
Contrôle #8 Gestion des sauvegardes	ISO/CEI 27002 12.3.1 Backups des informations
Contrôle #9 Gestion des mesures de protection	
Contrôle #10 Préparation des TIC pour la continuité des activités	ISO/CEI 27002 17.1.1 Planifier la continuité de la sécurité de l'information 17.1.2Assurer la continuité de la sécurité de l'information 17.1.3Vérifier, examiner et évaluer la continuité de la sécurité de l'information ISO/CEI 27 031 « Préparation des TIC pour la continuité des activités »
Contrôle #11 Télétravail	ISO/CEI 27002 6.2.1 Politique relative aux appareils mobiles 6.2.2 Télétravail
Contrôle #12 Surveillance des cybermenaces	
Contrôle #13 Sensibilisation à la sécurité de l'information	ISO/CEI 27002 7.2.2 Sensibilisation, éducation et formation en matière de sécurité de l'information
Contrôle #14 Sécurité de l'Information dans les relations avec les fournisseurs	ISO/CEI 27002 15.1.1 Politique de sécurité de l'information pour les relations avec les fournisseurs 15.1.2 Aborder la sécurité dans les accords avec les fournisseurs 15.1.3 Chaîne d'approvisionnement des technologies de l'information et de la communication 15.2.1 Suivi et révision des services fournisseurs 15.2.2 Gestion des changements apportés aux services des fournisseurs ISO/CEI 27036-1 « Sécurité de l'information pour les relations avec les fournisseurs — Partie 1 : Aperçu et concepts »
Contrôle #15 Organisation de la sécurité de l'information	ISO/CEI 27002 6.1.1 Rôles et sécurité de l'information 6.1.2 Séparation des tâches
Contrôle #16 Contrôles supplémentaires de la vie	ISO/CEI 27701

privée	

3 ANNEXE C : PROCESSUS COBIT ET GESTION DE LA SÉCURITÉ

Chacun des cinq domaines COBIT contient plusieurs processus. Tous ces processus comportent la structure suivante :

- Processus :
  - Description et but.
  - Objectifs de l'entreprise et paramètres.
  - Objectifs et paramètres informatiques.
- Pratiques de gestion :
  - Description de la pratique de gestion.
  - Mesures.
  - Tâches basées sur le niveau de capacité.
- Structures organisationnelles (matrice RACI).
- Flux et éléments d'information.
- Personnes, aptitudes et compétences.
- Politiques et procédures.
- Culture, éthique et comportement.
- Services, infrastructure et applications.

En suivant les étapes de cette méthodologie, nous serons en mesure de mettre en œuvre des contrôles de sécurité harmonisés avec la stratégie et les objectifs de l'entreprise. Nous obtiendrons également des renseignements très utiles sur l'efficacité des contrôles de sécurité.

Le tableau suivant montre les différents domaines et processus COBIT, et leur correspondance avec l'ensemble des contrôles de sécurité les plus utilisés en Europe, la norme ISO/CEI 27001 : 2013.

PROCESSUS COBIT		**ISO/CEI 27001**
EDM	**Évaluer, diriger et surveiller**	
	01 Établissement et maintenance du cadre de gouvernance	4.3 Déterminer la portée du système de management de la sécurité de l'information 5 Leadership 6.2 Objectifs de sécurité de l'information et planification pour les atteindre A.5 Politiques de sécurité de l'information
	02 Garantie des prestations	9.3 Révision par la direction 10 Amélioration
	03 Assurance de l'optimisation des risques	6.1 Mesures de gestion des risques et des possibilités 8.2 Évaluation des risques liés à la sécurité de l'information 8.3 Traitement des risques liés à la sécurité de l'information

	04 Assurance d'optimisation des ressources	7.1 Ressources 7.2 Compétence 7.3 Sensibilisation 7.5 Information documentée A.6.1 Organisation interne
	05 Assurance de la mobilisation des parties prenantes	4.1 Comprendre l'organisation et son contexte 4.2 Comprendre les besoins et les attentes des parties intéressées 7.4 Communication
APO	**Aligner, planifier et organiser**	
	01 Management du cadre de gestion des TIC	4.4 Système de gestion de la sécurité de l'information 5 Leadership A.5 Politiques de sécurité de l'information 8.1 Planification et contrôle opérationnels
	02 Gestion de la stratégie	4.4 Système de gestion de la sécurité de l'information 6.2 Objectifs de sécurité de l'information et planification pour les atteindre
	03 Gestion de l'architecture d'entreprise	A.9 Contrôle des accès A.11 Sécurité physique et environnementale A.12 Sécurité des opérations A.13 Sécurité des communications
	04 Gestion de l'innovation	
	05 Gestion du portefeuille	
	06 Gestion du budget et des coûts	8.3 Traitement des risques liés à la sécurité de l'information
	07 Gestion des ressources humaines	7.1 Ressources 7.2 Compétence 7.3 Sensibilisation A.7 Sécurité des ressources humaines
	08 Gestion des relations	4.2 Compréhension des besoins et des attentes des parties intéressées 7.4 Communication A.6.1 Organisation interne
	09 Gestion des Ententes de services gérées	4.2 Compréhension des besoins et des attentes des parties intéressées 7.4 Communication A.15 Relations avec les fournisseurs
	10 Gestion des fournisseurs	A.13.2 Transfert d'information A.14 Acquisition, développement et entretien des systèmes A.15 Relations avec les fournisseurs A.18.1.1 Identification des lois et des exigences contractuelles applicables A.18.1.4 Intimité et protection des informations relatives aux personnes identifiables
	11 Gestion de la qualité	9 Évaluation de la performance 10 Amélioration

	12 Gestion des risques	6.1 Actions pour adresser les risques et les possibilités 8.2 Évaluation des risques liés à la sécurité de l'information 8.3 Traitement des risques liés à la sécurité de l'information
	13 Management de la sécurité	Traité tout au long de la norme ISO/CEI 27001
	14 Gestion des informations	A.8 Gestion d'actifs A.10 Cryptographie A.12 Sécurité des opérations A.18.1.4 Intimité et protection des informations relatives aux personnes identifiables
BAI	**Construire, acquérir et mettre en œuvre**	
	01 Gestion des programmes	
	02 Gestion de la définition des exigences	4.2 Compréhension des besoins et des attentes des parties intéressées
	03 Gestion de l'Identification et de l'élaboration des solutions	A.14 Acquisition, développement et entretien des systèmes
	04 Gestion de la disponibilité et de la capacité	A.12.1.3 Gestion des capacités
	05 Gestion du changement organisationnel	A.12.1.2 Gestion du changement
	06 Gestion des changements des TIC	A.12.1.2 Gestion du changement
	07 Gestion de l'acceptation des changements et transition des TIC	A.12.1.2 Gestion du changement A.14 Acquisition, développement et entretien des systèmes
	08 Gestion des connaissances	7.5 Information documentée A.12.1.1 Procédures d'exploitation documentées A.16.1.6 Tirer des leçons des incidents de sécurité de l'information
	09 Gestion des actifs	A.8 Gestion des actifs
	10 Gestion de la configuration	A.9 Contrôle des accès A.12 Sécurité des opérations
	11 Gestion de la qualité	9 Évaluation des performances 10 Amélioration
DSS	**Prestation, service et soutien**	
	01 Gestion des opérations	8.1 Planification et contrôle opérationnels
	02 Gestion des demandes de service et des incidents	A.16 Gestion des incidents de sécurité de l'information
	03 Gestion des problèmes	A.16 Gestion des incidents de sécurité de l'information
	04 Gestion de la continuité	A.17 Aspects des activités liés à la continuité de la sécurité de l'information
	05 Gestion des services de sécurité	Traité tout au long de la norme ISO/CEI 27001
	06 Gestion des contrôles des processus opérationnels	9 Évaluation de la performance

MEA	Surveiller, évaluer et évaluer	
	01 Surveillance de la performance et de la conformité	9,1 Surveillance, mesure, analyse et évaluation 9.3 Revue par la direction
	02 Gestion du système de contrôle interne	9.2 Audit interne 4.2 Compréhension des besoins et des attentes des parties intéressées A.18 Conformité
	03 Gestion de la conformité aux exigences externes	9.2 Audit interne 4.2 Compréhension des besoins et des attentes des parties intéressées A.18 Conformité
	04 Gestion de l'assurance	9.3 Révision par la direction

4 ANNEXE D : LISTE DES ÉQUIPES D'INTERVENTION D'URGENCE INFORMATISÉES

Pays	Nom
Autriche	CERT.at (CERT national autrichien)
Belgique	Centre for Cyber Security Belgium
Bulgarie	Centre national bulgare d'intervention en matière de sécurité de l'information
Chypre	CSIRT-CY national
Danemark	Centre de cybersécurité (CCSC)
Estonie	CERT-EE (CERT national estonien)
Finlande	Centre national finlandais de cybersécurité
France	Agence nationale de cybersécurité, en anglais
Allemagne	CERT-Bund (CERT allemand), lien 2
Grèce	CSIRT hellénique
Hongrie	Centre national de cybersécurité de Hongrie
Irlande	IRISS
Italie	Agence nationale italienne de cybersécurité
Lettonie	Établissement d'intervention en cas d'incident lié à la sécurité des technologies de l'information
Malte	Gouvernement CSIRT de Malte
Pologne	CERT POLSKA (CERT polonais)
Portugal	Centre national portugais de cybersécurité
Roumanie	Direction nationale roumaine de la cybersécurité
Slovénie	SI-CERT (CERT national slovène)
Espagne	Institut national espagnol de cybersécurité
Suisse	Centre national suisse de cybersécurité
Pays-Bas	Dutch Digital Trust Centre
Royaume-Uni	Centre national de cybersécurité du Royaume-Uni

5 RÉFÉRENCES

ENISA (2015). *National/governmental CERTs – ENISA's recommendations on baseline capabilities*. ENISA. Retrieved from https://www.enisa.europa.eu/publications/national-governmental-certs-enisas- recommendations-on-baseline-capabilities

European Commission. (2020). E*urope's Digital Decade: digital targets for 2030. Brussels: European Commission*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes- digital-decade-digital-targets-2030_en (Retrieved December 21, 2021).

Eurostat. (2019). *ICT security in EU enterprises*. https://ec.europa.eu/eurostat/statistics-explained/ index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises (Retrieved December 21, 2021).

ISACA. (2019). *COBIT for Small and Medium Enterprises Using COBIT 2019*. ISACA.

International Organization for Standardization. (2021, December 21). I*SO 9000 FAMILY*

QUALITY MANAGEMENT. International Organization for Standardization. https://www.iso.org/iso-9001- quality-management.html

International Organization for Standardization. (2020). *Information security, cybersecurity and privacy protection — Governance of information security*. (ISO/IEC 27014:2020). https://www.iso.org/standard/ 74046.html

International Organization for Standardization. (2019). *Security techniques — Extension to ISO/IEC27001 and ISO/IEC 27002 for privacy information management — Requirements a nd guidelines.* (ISO/IEC 27701:2019). https://www.iso.org/standard/71670.html

International Organization for Standardization. (2018). *Information technology — Security techniq ues — Information security risk management*. (ISO/IEC 27005:2018). https://www.iso.org/standard/75281.html

International Organization for Standardization. (2015). *Conformity assessment — Require ments for bodies providing audit and certification of management systems — Part 1: Requ irements*. (ISO/IEC 17021-1:2015). https://www.iso.org/standard/61651.html

International Organization for Standardization. (2013). *Information technology — Security techniq ues — Information security management systems — Requirements*. (ISO/IEC 27001:2013). https://

www.iso.org/ standard/54534.html

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security controls*. (ISO/IEC 27002:2022). https://www.iso.org/standard/75652.html

International Organization for Standardization. (2013). *Information technology — Security techniques — Code of practice for information security controls*. (ISO/IEC 27002:2013). https://www.iso.org/standard/ 54533.html

International Organization for Standardization. (2012). *Conformity assessment — Require ments for bodies certifying products, processes and services*. (ISO/IEC 17065:2012). https:/ /www.iso.org/standard/ 46568.html

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. In *ARES 2021: The 16th International Conference on Availability, Reliability and Security* (pp. 1-7). Vienna; Association for Computing Machinery. Retrieved 21 December 2021, from htt ps:// dl.acm.org/doi/pdf/10.1145/3465481.3469200.

Regulation (EU) 2016/679. *The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. European Parliament, Council of the European Union. https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:32016R0679

Small Business Standards (SBS). (2017). *SME Guide for the Implementation of ISO/IEC 270 01 on Informat ion Security Management*. Brussels: SBS. Retrieved from https://www.sbs-sme.eu/publication/sme-guide-implementation-iso-iec-27001-information-security-management

6 À PROPOS DES EXPERTS

Président : Jean-Luc Allard
Ingénieur industriel, CISM (à la retraite). Ancien officier de l'armée de l'air belge. Expert en gouvernance et gestion de la sécurité de l'information avec 25 ans d'expérience. Actif dans la normalisation (ISO/IEC JTCI SC27) depuis 2002.
Consultant indépendant en gouvernance et gestion de la sécurité des formations.

Coordinateur : Omar Dhaher
Senior Technology Manager chez DIGITAL SME. Coordinateur du DIGITAL SME WG Standards et du WG SBS Digitalisation. Membre de la Task Force Rolling Plan du Multi Stakeholders Platform de la Commission Européenne sur la normalisation des TIC. Expérience des TIC, de la politique industrielle dans son rapport aux cadres réglementaires des télécommunications, de l'esprit d'entreprise, de l'apprentissage en milieu de travail, des compétences numériques, de la recherche et de la normalisation.

Membres

Andrea Caccia
Consultant Senior, gestionnaire de projet, conformité aux normes et aux règlements, coordonnateur du développement de produits sur :
Services de confiance et tous produits et technologies connexes, p. ex : signature électronique, eSeal et eDelivery
Facturation et archivage électroniques
blockchain et DLT
Andrea participe aux plus importantes activités de normalisation européenne (ETSI, CEN, ISO, UNI/ UNINFO, OASIS)

Daniele Tumietto
Consultant indépendant, conseiller senior, manager de l'innovation. Daniele est également professeur adjoint à l'Université Link Campus de Rome (Italie) et à l'Université O.M. Beketov de Kharkiv (Ukraine).
Daniele est membre de plusieurs comités techniques de normes nationales, européennes et internationales en facturation électronique, approvisionnement électronique, commerce électronique et services financiers, eIDAS, protection de la vie privée et des données personnelles, blockchain & DLT, industrie 4.0, technologies quantiques, IA, économie circulaire et ESG.

Davide Giribaldi
CEO de EnCybeRisk srl — Senior GRC et conseiller en sécurité de l'information — coordinateur du Groupe de travail sur la cybersécurité d'Assintel avec une connaissance approfondie dans le domaine de la gestion des risques liés à la sécurité d'entreprise. Davide possède 27 ans d'expérience dans des contextes critiques, afin d'assurer la continuité des activités et la gestion des crises pour les organismes publics italiens et les grandes multinationales.

Francisco Menéndez
Francisco est spécialiste de la sécurité de l'information, de la gestion des services et de la continuité des activités et chef des services de sécurité de l'information et de conformité chez Seresco. Il est auditeur principal pour les normes ISO 27001, 28 000, 20000-1 et 22 301. Membre Platinum de ISACA. Certifications ISACA : CISA, CISM, CRISC et COBIT Foundation. Francisco est le coordinateur et membre du groupe de travail itSMF Espagne et membre du groupe de travail Centre de cybersécurité industrielle.

Samuel Fricker

Professeur à l'Université des sciences appliquées du nord-ouest de la Suisse et coordinateur du projet Horizon-2020 GEIGER[1]. Le GEIGER[18] vise à apporter la cybersécurité aux petites et moyennes entreprises en coopération avec European DIGITAL Alliance SME, l'ENISA, l'ECSO et divers acteurs nationaux. Samuel est titulaire d'un doctorat de l'Université de Zurich.

[18] Les contributions apportées par le projet GEIGER à ce guide ont reçu un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne au titre de l'accord de subvention no 883588.

Small Business Standards

sbs-sme.eu

@SBS_SME

European DIGITAL SME Alliance

digitalsme.eu

@EUdigitalsme

Cofinancement par la Commission européenne et les États membres de l'AELE

Ce guide reflète les points de vue des PME. La Commission européenne et les États membres de l'AELE ne sont pas en mesure de fournir les informations nécessaires.