Haute École
Groupe ICHEC – ECAM – ISFSC

Enseignement supérieur de type long de niveau universitaire

Comment promouvoir et se conformer à la directive NIS 2 ? Étude de cas Agoria

Mémoire présenté par :

Amir OULAD HAJ AMAR

Pour l'obtention du diplôme de :

Master en gestion de l'entreprise

Année académique 2023-2024

Promotrice :

Thanh-Diane NGUYEN

Boulevard Brand Whitlock 6 - 1150 Bruxelles

Remerciement

En préambule, je voudrais exprimer ma profonde gratitude envers plusieurs personnes sans lesquelles ce mémoire n'aurait pas pu voir le jour tel qu'il est aujourd'hui.

Tout d'abord, j'aimerais remercier ma promotrice, Madame Thanh-Diane NGUYEN, pour sa disponibilité constante et ses conseils avisés. Grâce à son enseignement, j'ai pu découvrir et m'immerger dans le domaine passionnant de la gouvernance et des technologies de l'information, ce qui m'a ouvert la voie vers la réalisation de ce travail.

Ensuite, je tiens à exprimer ma reconnaissance envers toutes les personnes qui ont accepté de m'accorder des interviews. Leur patience et leur volonté de partager leurs connaissances ont été inestimables pour l'élaboration de mes recherches finales. Sans leur collaboration, ce mémoire n'aurait pas pu être aussi complet et pertinent.

Je remercie également mon maître de stage, Eric Van Cangh, pour son aide précieuse et ses conseils tout au long de mon stage. Son soutien, ainsi que la documentation et les opportunités de réseautage qu'il m'a offertes, ont été essentiels à l'écriture de ce mémoire.

Enfin, je souhaite exprimer toute ma gratitude envers mes proches, et en particulier mes parents. Leur soutien indéfectible tout au long de mes études et de ma vie a été une source inestimable de motivation et de force. Je suis l'homme que je suis aujourd'hui grâce à eux.

Merci à tous pour votre aide et votre soutien.

Engagement anti-plagiat et respect des règles

« Je soussigné, OULAD HAJ AMAR Amir, en Master 2, déclare par la présente que le mémoire ci-joint est exempt de tout plagiat et respecte en tous points le règlement des études en matière d'emprunts, de citations et d'exploitation de sources diverses signé lors de mon inscription à l'ICHEC, ainsi que les instructions et consignes concernant le référencement dans le texte respectant la norme APA, la bibliographie respectant la norme APA, etc. mises à ma disposition sur Moodle.

Sur l'honneur, je certifie avoir pris connaissance des documents précités et je confirme que le Mémoire présenté est original et exempt de tout emprunt à un tiers non-cité correctement. »

« Je soussigné, OULAD HAJ AMAR, Amir, en Master 2, déclare par la présente que le travail ci-joint respecte les règles de référencement des sources reprises dans le règlement des études en signé lors de mon inscription à l'ICHEC (respect de la norme APA concernant le référencement dans le texte, la bibliographie, etc.) ; que ce travail est l'aboutissement d'une démarche entièrement personnelle; qu'il ne contient pas de contenus produits par une intelligence artificielle sans y faire explicitement référence. Par ma signature, je certifie sur l'honneur avoir pris connaissance des documents précités et que le travail présenté est original et exempt de tout emprunt à un tiers non-cité correctement. » 20 Mai 2024

Je soussigné(e), Oulad Haj Amar 190246 (nom + numéro de matricule), déclare sur l'honneur les éléments suivants concernant l'utilisation des intelligences artificielles (IA) dans mon travail / mémoire :

Type d'assistance		Case à cocher
Aucune assistance	J'ai rédigé l'intégralité de mon travail sans avoir eu recours à un outil d'IA générative.	
Assistance avant la rédaction	J'ai utilisé l'IA comme un outil (ou moteur) de recherche afin d'explorer une thématique et de repérer des sources et contenus pertinents.	
Assistance à l'élaboration d'un texte	J'ai créé un contenu que j'ai ensuite soumis à une IA, qui m'a aidé à formuler et à développer mon texte en me fournissant des suggestions.	
	J'ai généré du contenu à l'aide d'une IA, que j'ai ensuite retravaillé et intégré à mon travail.	
	Certains parties ou passages de mon travail/mémoire ont été entièrement été générés par une IA, sans contribution originale de ma part.	
Assistance pour la révision du texte	J'ai utilisé un outil d'IA générative pour corriger l'orthographe, la grammaire et la syntaxe de mon texte.	X
	J'ai utilisé l'IA pour reformuler ou réécrire des parties de mon texte.	X
Assistance à la traduction	J'ai utilisé l'IA à des fins de traduction pour un texte que je n'ai pas inclus dans mon travail.	
	J'ai également sollicité l'IA pour traduire un texte que j'ai intégré dans mon mémoire.	
Assistance à la réalisation de visuels	J'ai utilisé une IA afin d'élaborer des visuel, graphiques ou images.	
Autres usages		

Je m'engage à respecter ces déclarations et à fournir toute information supplémentaire requise concernant l'utilisation des IA dans mon travail / mémoire, à savoir :

J'ai mis en annexe les questions posées à l'IA et je suis en mesure de restituer les questions posées et les réponses obtenues de l'IA. Je peux également expliquer quel le type d'assistance j'ai utilisé et dans quel but.

Fait à Bruxelles (ville), le 20 mai 2024 (date)

Signature : Amir Oulad Haj Amar 190246 [Prénom Nom de l'étudiant(e) et matricule]

« Face au monde qui change, il vaut mieux penser le changement que changer le pansement. »

Francis Blanche

Table des matières

Table des figures et tableaux :

Section 1 : Introduction

1.1 Contexte du problème

Dans le paysage numérique contemporain, où la technologie évolue à une vitesse fulgurante et où les données constituent le pilier central des entreprises, la cybersécurité est devenue une préoccupation omniprésente. Les organisations, quel que soit leur secteur, sont confrontées à des menaces numériques en constante mutation qui mettent en péril la sécurité de l'information. Avec l'émergence de technologies avancées telles que l'intelligence artificielle, les IA génératives et une adoption accrue du cloud computing, les organisations doivent non seulement protéger leurs infrastructures contre les cyberattaques comme le ransomware et le phishing, mais également contre les risques internes.

Cependant, la cybercriminalité ne connaît pas de frontières, et la Belgique n'est pas épargnée par cette menace. En tant que centre politique de l'Europe, abritant de nombreuses institutions de l'Union européenne ainsi que l'OTAN, la Belgique se trouve particulièrement exposée aux cyberattaques visant à perturber ses fonctions gouvernementales et à compromettre la sécurité des informations. Le Centre pour la Cybersécurité Belgique (CCB) a signalé une augmentation significative du nombre d'incidents de cybersécurité ces dernières années, mettant en lumière la nécessité d'une vigilance et d'une préparation accrues face à ces menaces (CCB, 2024-b).

En effet, les attaques par ransomware, un logiciel malveillant qui prend en otage les données est parmi les menaces les plus répandues, ce qui a paralysé les opérations et exigé des rançons importantes. La durée moyenne d'activation d'un ransomware est passée de 5,5 jours en 2020 à moins de 24 heures en 2022, démontrant leur agilité. (Filippone, 2023)

De plus, les attaques de phishing ont également gagné en sophistication, utilisant des techniques d'ingénierie sociale pour tromper même les utilisateurs avertis. Ces attaques regroupent l'ensemble des techniques utilisées pour voler des informations sensibles en s'appuyant sur les réactions de tout un chacun face à une urgence, une menace ou une situation inhabituelle. En se faisant passer pour une banque, un organisme officiel, un opérateur mobile ou un site de vente en ligne, les pirates contactent ses utilisateurs pour demander de leur transmettre des informations confidentielles : mots de passe, moyens de paiement, identité, données professionnels… Durant le premier trimestre de 2023, 562,4 millions de mails de phishing ont été détectés. (Orange Corporate, s.d.).

Les menaces internes, qu'il s'agisse de négligence innocente ou de comportement malveillant, sont devenues une source majeure de préoccupations en matière de sécurité de l'information. En effet, 74 % des brèches impliquent une erreur humaine. (Orange Corporate, s.d.).

Face à ce contexte, l'adoption de mesures robustes pour combattre la cybercriminalité est devenue une priorité pour de nombreux pays, y compris la Belgique. Agoria se situe au cœur de cet environnement complexe. En tant qu'acteur majeur dans le secteur technologique, Agoria joue un rôle crucial dans la sensibilisation et la mise en œuvre des meilleures pratiques de cybersécurité. La nécessité pour les organisations de renforcer leur cybersécurité est devenue plus pressante avec l'introduction de la directive NIS 2 de l'UE, qui vient renforcer et élargir les exigences de la directive originale NIS. La directive NIS, adoptée pour améliorer la résilience des réseaux et des systèmes d'information à travers

l'UE, a posé les fondements d'une coopération renforcée entre les États membres face aux cybermenaces. NIS 2, en étendant le champ d'application et en imposant des obligations plus strictes en matière de sécurité et de reporting des incidents, met en évidence l'importance accrue de la cybersécurité dans l'agenda réglementaire européen.

Les régulateurs du monde entier ont intensifié leurs efforts pour protéger les consommateurs et assurer la stabilité des infrastructures critiques en imposant des normes de conformité de plus en plus strictes en matière de sécurité des informations et de protection des données. Les organisations sont donc confrontées à une avalanche de réglementation. Elles se retrouvent submerger, parfois, se sentir dépassées, voire menacées de paralysie, face à la nécessité d'adapter rapidement leurs pratiques.

Dans ce contexte tumultueux, la sensibilisation, la promotion et l'accompagnement des entreprises revêtent une importance capitale. Il est crucial de fournir aux organisations les outils et les connaissances nécessaires pour déchiffrer et se conformer efficacement aux réglementations en vigueur. Ainsi, le rôle des fédérations et des organismes sectoriels, tels qu'Agoria, est essentiel pour garantir que les entreprises puissent continuer à opérer efficacement tout en respectant les cadres réglementaires en perpétuelle mutation.

1.2 Question de recherche

Dans une ère caractérisée par la transformation numérique et la croissance des risques, sensibiliser les entreprises à l'importance de la cybersécurité est devenu impératif. La question centrale de ma recherche s'attaque à la nécessité de faire comprendre et adopter cette directive cruciale par les acteurs économiques. Ma question est donc la suivante :

« Comment promouvoir et se conformer à la directive NIS 2 ? » Étude de cas Agoria

L'étude de cas d'Agoria, la fédération de la technologie en Belgique, fournira des insights précieux sur les meilleures pratiques en matière de sensibilisation à la cybersécurité. En déchiffrant la dynamique et les stratégies d'Agoria, ce mémoire cherche à explorer les mécanismes par lesquels les entreprises peuvent non seulement se conformer à la législation, mais aussi jouer un rôle actif dans la promotion d'une culture de la sécurité numérique robuste et résiliente.

Cette problématique guide l'exploration des stratégies et des mécanismes que les organisations peuvent déployer pour atteindre une conformité fluide avec la directive NIS 2. Elle implique également de se pencher sur les opportunités offertes par cette intégration, telle que l'amélioration de la résilience organisationnelle, l'alignement avec les meilleures pratiques internationales, et la valorisation de la confiance des clients dans un marché numérique de plus en plus réglementer.

Ce choix d'axe d'étude est motivé par l'urgence pour les entreprises de revisiter leurs stratégies de cybersécurité existantes pour les aligner sur les nouveaux standards européens comme depuis l'entrée de la directive en 2023. Avec des menaces telles que le ransomware et le phishing qui évoluent rapidement, et la reconnaissance que les erreurs humaines restent une cause prédominante des brèches de sécurité, les organisations doivent maintenant naviguer entre la nécessité d'une protection robuste et la conformité réglementaire stricte. La directive NIS 2, avec son champ d'application élargi et ses exigences accrues, représente un tournant dans la réglementation européenne en matière de sécurité de

l'information. En choisissant d'examiner les défis et opportunités pour les organisations dans l'adoption de cette directive, ce mémoire vise à élucider comment les cadres de gouvernance peuvent être intégrés de manière effective pour non seulement répondre aux exigences réglementaires, mais également pour renforcer la posture de sécurité globale.

L'intérêt de cette hypothèse se reflète aussi dans l'identification des meilleures pratiques et en mettant en lumière les leçons tirées de l'intégration des directives de la NIS 2, les organisations peuvent aspirer à une sécurité renforcée, à une réputation solide, et finalement, à une valeur accrue dans l'économie numérique. Ce mémoire ambitionne donc de fournir un cadre analytique et des recommandations stratégiques pour aider les entreprises à naviguer dans ce paysage réglementaire complexe, en transformant les défis en leviers de croissance et d'innovation.

1.3 Introduction de l'entreprise

Agoria est une fédération industrielle de premier plan en Belgique, axée sur le secteur technologique. Fondée en 1946 initialement sous le nom de Fabrimetal, cette organisation avait pour vocation de représenter les intérêts des entreprises actives dans les secteurs de la métallurgie, de la construction électrique et de la plasturgie. Issue de la Fédération des Constructeurs de 1906, Fabrimetal a connu son apogée en regroupant jusqu'à 1.200 entreprises.

Le 9 novembre 2000, la fédération a opéré une transformation significative en changeant son nom pour Agoria, marquant ainsi une évolution vers une portée plus étendue incluant des entreprises au-delà du secteur de la métallurgie, notamment dans les TIC, reflétant les changements dans la pratique et la vision de l'industrie.

Aujourd'hui, Agoria est une fédération belge qui « ... ouvre la voie à toutes les entreprises belges inspirées par la technologie, qui développent et commercialisent des solutions durables pour réaliser la croissance et le progrès dans le monde entier. Elle représente plus de 2.100 entreprises technologiques belges, 70% sont des PME, allant des secteurs manufacturier et numérique jusqu'aux télécommunications. À elle seule elle représente approximativement 324.000 employés. Elle est le plus grand membre de la Fédération des entreprises de Belgique (FEB), affirmant sa position centrale dans l'écosystème industriel belge. (Agoria, s-d.).

Avec environ 200 employés et des bureaux répartis dans les principales villes belges, Agoria se positionne comme un acteur clé pour le soutien et la promotion du secteur technologique en Belgique. Elle a pour but de les de connecter tout le monde via la technologie et l'innovation. On peut la voir comme le point médian entre le gouvernement, la défense, les entreprises et les nouveaux talents représentés par les écoles.

La structure d'Agoria est assez complexe, mais voici un petit résumé qui devrait faciliter la compréhension de ses activités quotidiennes. Les deux principaux axes sont le « Digital » et la « Fabrication », chacun ayant des responsables différents, Saskia Van Uffelen représentant la partie numérique et Ben Van Roose, son équivalent pour la fabrication, et comprenant différentes équipes. Chacun a des Leaders de Groupes d'Affaires (BGL) ayant chacun leur domaine de prédilection. Ferdinand Casier (IA), Floriane de Kerchove (Talents), Eric Van Cangh (Cybersécurité) ... sont tous des Leaders de Groupes d'Affaires dans le département Digital. Alors qu'Alain Wayenberg (ICS/OT) et Georges Heeren (défense) représentent des Leaders de Groupes d'Affaires dans l'équipe de Fabrication.

À l'intérieur de ces deux départements, deux sous-départements appelés « Services » et « Contexte » existent. Alors que les Services se concentrent davantage sur les aspects techniques pratiques, le Contexte concerne davantage les relations avec les membres, le réseautage, l'organisation d'événements et bien plus encore.

Cyber Made in Belgium (CMiB), est une subdivision importante d'Agoria, c'est la voie de l'industrie de la cybersécurité en Belgique.

Outre son rôle de représentation et de plaidoyer, Agoria joue également un rôle crucial dans l'innovation technologique grâce à son centre technologique, Sirris. Ce dernier fournit un soutien aux entreprises pour l'intégration de nouvelles technologies dans leurs produits, processus et opérations.

Le secteur technologique en Belgique, représenté par Agoria, se distingue par sa forte valeur ajoutée et sa croissance économique, avec une valeur ajoutée de 39 milliards d'euros en 2019 et une croissance économique réelle de 11,5 % depuis 2015. Le chiffre d'affaires du secteur atteignait 132 milliards d'euros en 2019, avec des investissements dépassant les 4 milliards d'euros, témoignant de la vitalité et de l'importance du secteur technologique dans l'économie nationale.

1.4 Méthodologie et Limites

Tout au long de ce parcours, j'ai significativement enrichi mes connaissances dans le domaine de la cybersécurité, notamment en ce qui concerne la directive NIS 2, grâce à une série d'initiatives personnelles et d'engagements professionnels. Ma participation active à plusieurs séminaires tels que le Forum in Cyber à Lille (FIC), des bootcamps, ainsi que des sessions de networking et discussions informelles avec des experts dans le domaine, m'ont permis de plonger dans les complexités de cette directive européenne critique.

Ces interactions ont été particulièrement enrichissantes et m'ont ouvert les yeux sur l'importance stratégique de la directive NIS 2 pour les entités opérant dans l'Union européenne. Les échanges avec des professionnels et des spécialistes de la cybersécurité, lors de ces événements, ont souligné l'urgence et la nécessité pour les organisations de renforcer leur posture de sécurité.

En outre, ces interactions m'ont permis de comprendre plus profondément les perspectives variées sur la gestion des risques de cybersécurité, l'importance de la culture de la sécurité dans l'entreprise et les meilleures pratiques pour une mise en œuvre réussie de la directive. Grâce à ces apprentissages, j'ai pu adopter une approche plus éclairée et critique pour l'élaboration de ce mémoire, qui vise à explorer non seulement les exigences de la NIS 2, mais aussi les stratégies optimales pour sa mise en place efficace.

Ce mémoire est donc le fruit d'une démarche d'enrichissement continu, marquée par un engagement actif dans le domaine de la cybersécurité, et inspirée par les insights et les recommandations de leaders et d'experts reconnus.

Mon mémoire se penche donc sur la cybersécurité sous l'angle de la directive NIS 2, en mettant l'accent sur les actions que les entreprises pourraient entreprendre pour se conformer et les implications de ces mesures. La méthodologie que suit le mémoire consistera à suivre le schéma suivant :

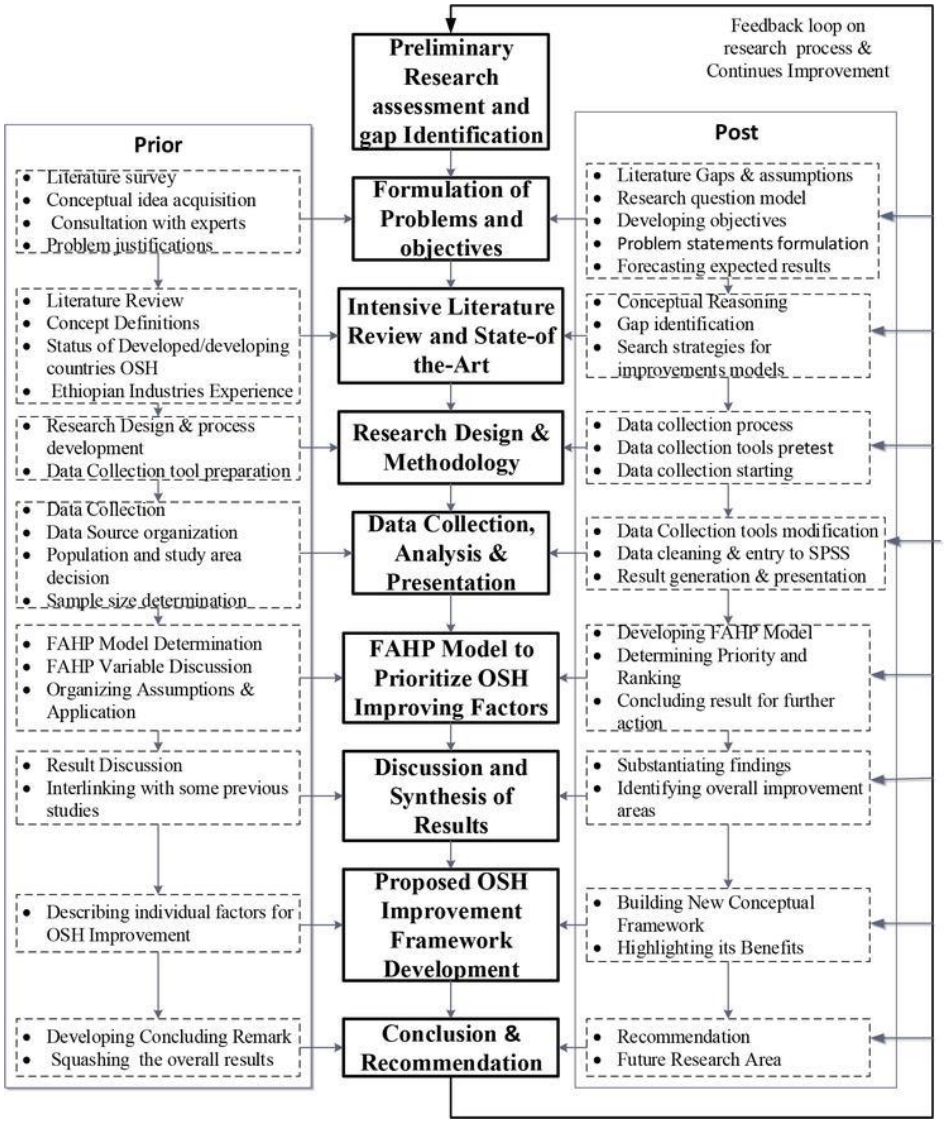


Figure 1: Research design

Source: Sileyew, K. J. (2020). *Research Design and Methodology*. Dans IntechOpen eBooks. https://doi.org/10.5772/intechopen.85731

Le travail débute par une revue préliminaire de la littérature afin d'identifier les problématiques liées à la cybersécurité et à la directive NIS 2. Cette étape permet de se familiariser avec les concepts et le contexte, avant de formuler une question de recherche qui guidera le mémoire.

Ensuite, une analyse exploratoire approfondie est menée pour identifier le cadre théorique nécessaire à la compréhension des concepts et des variables en jeu, ainsi que pour contextualiser la recherche dans les travaux existants. Cette revue de littérature s'appuie sur une diversité de sources telles que des ressources en ligne, des bibliothèques, des articles de presse et des études sectorielles. Les contributions d'autorités réglementaires et d'organisations telles que le CCB, la Cyber Security Coalition et Agoria ont également enrichi cette revue de littérature.

En parallèle de cette analyse théorique, une étude de cas est effectuée pour illustrer et présenter les initiatives mises en place par Agoria pour promouvoir la cybersécurité et sensibiliser les entreprises

belges à l'importance de cette directive. La promotion de la cybersécurité en Belgique est un aspect crucial dans le contexte de la mise en œuvre de la directive NIS 2.

Pour collecter des données et les analyser par la suite j'ai opté pour une combinaison des deux méthodes. D'abord la quantitative, en concevant un questionnaire composé de plusieurs questions sur la directive NIS 2. L'objectif de ce questionnaire était de collecter des données quantitatives directement auprès des entreprises concernées par cette réglementation, afin d'évaluer leur niveau de connaissance, de préparation et de conformité à la directive.

Pour la réalisation de ce questionnaire, j'ai bénéficié de l'assistance de Patrick Slaets, expert chez Agoria en études et en Data. Il m'a donné des conseils sur la diffusion du questionnaire et sur la formulation des questions afin d'atteindre un maximum de personnes et d'obtenir des réponses pertinentes. (Annexe 1)

Malheureusement, j'ai rencontré une limite qui m'a empêché de partager mon questionnaire. Agoria travaillait en même temps sur un projet européen nommé "CyberHubs" qui comprenait un questionnaire sur les compétences et les profils recherchés en cybersécurité au sein de ses entreprises membres. Ils ne pouvaient donc pas partager deux questionnaires simultanément, car cela aurait été trop pour les personnes interrogées. Étant donné que mon questionnaire visait à évaluer les connaissances et la sensibilisation des personnes par rapport à la directive NIS 2, et que le public cible était le même, il était impossible de le partager.

L'intégration de cette recherche quantitative aurait enrichi l'analyse de mon mémoire en fournissant des données concrètes sur l'état actuel de la conformité et des défis liés à la mise en œuvre de la directive NIS 2 au sein des entreprises.

En complément de ma démarche méthodologique axée sur la recherche quantitative, j'ai élaboré une approche qualitative. Cette recherche qualitative a été réalisée à travers des entretiens semi-dirigés avec des experts et des professionnels du domaine de la cybersécurité.

L'objectif principal de ces entretiens est de recueillir des informations détaillées sur comment mener à bien une conduite du changement dans le cadre de l'implémentation de la directive NIS 2. En menant ces entretiens, je cherche à identifier les limites et difficultés auxquelles une entité pourrait faire face ainsi que la complexité du changement pour ensuite donner une feuille de route sur les pratiques à avoir.

La sélection des participants à ces entretiens s'est appuyée sur mon réseau professionnel dans le domaine de la cybersécurité, ainsi que sur les contacts établis lors de mes précédentes recherches et collaborations. Je chercherai à inclure une diversité de perspectives, en engageant des experts provenant de différents secteurs d'activité et ayant des niveaux variés d'expérience en matière de cybersécurité et de conformité réglementaire.

Les entretiens sont structurés autour de thèmes clés identifiés à partir de l'analyse exploratoire, tout en laissant également la place à des discussions ouvertes pour permettre l'émergence de nouvelles idées et perspectives. J'ai donc réalisé des guides d'entretien avec plusieurs questions divisées en thème.

J'ai pu avoir des interviews cruciales et nécessaires à la bonne construction de mon travail.

- La première discussion était celle avec Arnaud MARTIN d'Agoria. Il me semblait tout d'abord essentiel de comprendre les subtilités de la directive et le mieux placé pour cela était selon moi l'expert en standardisation et législation au sein d'Agoria. Arnaud est celui qui s'occupe

d'accompagner les membres d'Agoria dans leur conscientisation à cette directive. Il a également participé à des réunions pour la transposition de cette directive en Belgique. (Annexe 5 : Interview Arnaud Martin)

- La seconde interview était avec Valery VANDE GEETEN du centre de la cybersécurité en Belgique (CCB) qui est l'organisme en charge de la transposition de la directive en Belgique. On a pu discuter de la directive dans son ensemble, de l'origine ainsi que de son impact. (Annexe 6 : Interview Valery Vanden Geeten)
- La troisième discussion fut avec Floriane DE KERCHOVE qui fait du lobby et de l'advocacy chez Agoria. On a pu discuter des choses mises en place par la fédération ainsi que de problématique auxquels on faisait face ici en Belgique. (Annexe 7 : Interview Florianne De Kerchove)
- La quatrième discussion avec Eric VAN CANGH, maitre de stage et business group leader en cybersécurité chez Agoria. La discussion tournait également autour de la directive ainsi que de la promotion de la cybersécurité en Belgique ainsi qu'auprès des membres d'Agoria. (Annexe 8 : Interview Eric Van Cangh)
- La cinquième discussion était avec CyberWal qui est une entité dans le domaine de la cybersécurité en Wallonie créée par digital wallonia. La discussion était axée sur la problématique de la formation de talent. (Annexe 9 : Interview Cyberwal)
- La dernière discussion était avec deux consultants en cybersécurité au sein de NVISO j'ai eu la possibilité d'échanger avec eux sur le côté implémentation de la directive auprès des clients. J'ai pu avoir des insights sur les problématiques de la réalité du terrain. (Annexe 10 : Interview Nviso)

Les informations recueillies lors de ces entretiens sont ensuite analysées de manière qualitative, en mettant en évidence les motifs récurrents, les points de convergence et de divergence, ainsi que les insights significatifs pour enrichir l'interprétation des résultats de la recherche.

En intégrant cette approche qualitative, j'obtiens à la fois les données objectives sur le niveau de conformité des entreprises ainsi que les motivations, perceptions et expériences des acteurs clés du domaine. En intégrant ces deux aspects, j'ai pu obtenir une compréhension approfondie des défis rencontrés par les entreprises en matière de cybersécurité et des implications de la directive NIS 2.

En conclusion, cette méthodologie permet d'explorer les données théoriques en lien avec la cybersécurité, suivi d'un plan d'action sur le cas d'Agoria et sa promotion de la cybersécurité dans une grande mesure s'en suit l'analyse empirique de la mise en place de la directive dans les entités concernées et finalement des recommandations et conclusions seront fourni.

Section 2 : État de l’art

Pour aborder de manière approfondie l’étude sur la manière de sensibiliser les entreprises à la directive NIS 2, je débute avec un examen minutieux de l'état de l'art. Cette étape cruciale du mémoire vise à jeter les bases conceptuelles nécessaires pour une compréhension complète du sujet. Je commencerai par définir et clarifier plusieurs termes clés liés à la directive NIS 2 et à la cybersécurité. Ces définitions serviront de fondement à mon analyse, m’aidant à cerner les enjeux de manière précise et à formuler des réponses éclairées à ma question de recherche : comment sensibiliser les entreprises à la directive NIS 2 ? L'étude de cas centrée sur Agoria me permettra d'illustrer concrètement les stratégies et les défis associés à cette sensibilisation dans le contexte des entreprises belges.

2.1 Sécurité des systèmes d’information

2.1.1 Définition d’un système d’information

L'ensemble des méthodes et des moyens organisationnels, juridiques et humains utilisés pour protéger ou rétablir la disponibilité, la confidentialité et l'intégrité d'un système d'information est appelé sécurité du système d'information. L'une des principales parties de la protection des données est la sécurité. Les organisations doivent mettre en place des modèles et des processus de gestion des risques permettant d'apprécier les risques de sécurité liés au traitement des données à caractère personnel afin de garantir un niveau adéquat de protection. Après cela, ils doivent mettre en place des mesures de sécurité pour faire face aux risques. (SPF Economie, 2022).

En règle générale, les systèmes d'information s'appuient sur des systèmes informatiques pour leur mise en œuvre. Les données de télécommunications (voix analogique, voix sur IP…) et dans certains cas, les données sur papier.

2.1.2 Système d’information, cybersécurité et sécurité informatique : les différences ?

Bien que les termes « cybersécurité » et « sécurités des systèmes d'information » soient souvent utilisés de manière interchangeable, ils ne couvrent pas exactement la même réalité, car chacun correspond à différents types de sécurité.

La **sécurité informatique** est le processus global de protection des ressources informatiques, incluant les terminaux, bases de données, serveurs, réseaux, contre tout accès non autorisé. Son objectif est de prévenir les risques d'utilisation abusive ou de vol, que les menaces proviennent de l'intérieur ou de l'extérieur d'une entreprise. Ce processus englobe un ensemble de règles, procédures techniques et outils visant à garantir la confidentialité, l'intégrité et la disponibilité des données manipulées par les systèmes informatiques au quotidien. (European Data Protection Supervisor, s. d.).

La sécurité informatique se concentre principalement sur la composante technique du Système d'Information. En revanche, la Sécurité du Système d'Information (SSI) élargit son champ d'action en incluant les aspects humains et informationnels du Système d'Information (Figure 2). Elle prend en compte la sécurité de l'information sous des formes non numériques, telles que les documents papier et les connaissances. La SSI a pour mission de protéger la confidentialité, l'intégrité et la disponibilité des données en prévenant tout accès non autorisé, manipulation, ou destruction. (Direction du Système d'Information et des Usages Numériques, 2020).

En tant que sous-ensemble de la sécurité informatique, **la cybersécurité** se concentre principalement sur la protection contre les cyberattaques et les menaces d'Internet. Elle met l'accent sur l'importance de protéger les ressources contre les piratages et les attaques en ligne. En d'autres termes, la cybersécurité est la discipline qui se concentre sur la protection des systèmes, des réseaux et des données numériques contre les menaces et les attaques potentielles. Elle englobe des domaines tels que la sécurité des réseaux, la gestion des identités et des accès, la sécurité des applications et la gestion des incidents de sécurité. (Skandrani, 2023)

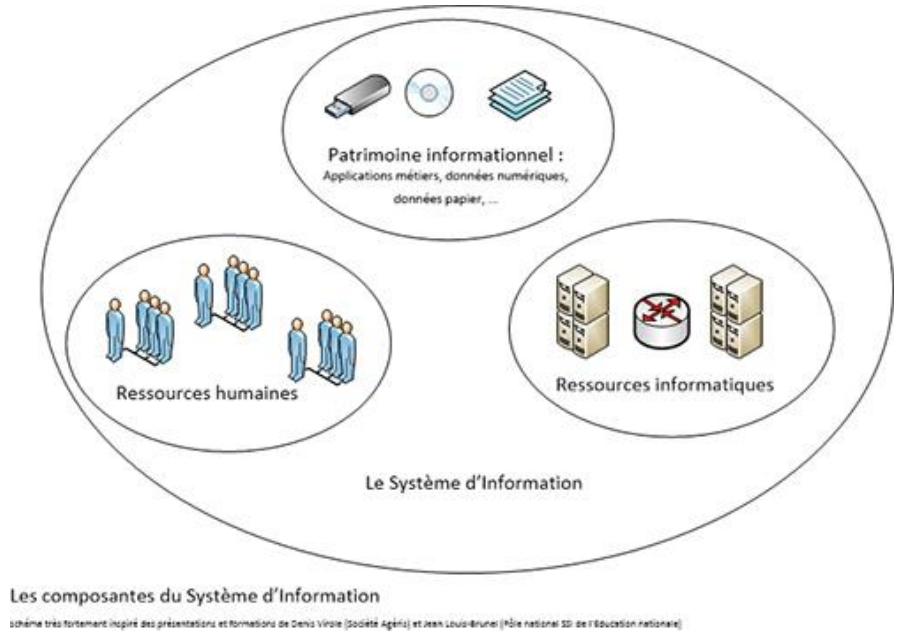


Figure 2: Les composantes du système d'information

Source : Direction du Système d'Information et des Usages Numériques. (2020, 29 septembre). La *Sécurité du Système d'Information* (SSI). Consulté le 20 novembre 2023, à l'adresse https://dsiun.univ-tln.fr/La-Securite-du-Systeme-d-Information-SSI.html

Exemple Concret :

- **Sécurité des systèmes d'information** : La société utilise des coffres-forts pour les documents financiers, des politiques de contrôle d'accès pour les employés et des sauvegardes régulières des données clients.
- **Cybersécurité** : Elle met en place des systèmes de détection des intrusions, des protocoles de chiffrement pour les transactions en ligne et des formations régulières en sécurité pour les employés.

Étude de Cas :
Lors d'une attaque récente de ransomware, une entreprise a pu récupérer rapidement ses données grâce à une bonne gestion de la sécurité des systèmes d'information (sauvegardes régulières). Cependant, l'incident a révélé une faille dans sa cybersécurité, car l'attaque initiale s'est faite via un courriel de phishing non détecté. Cela illustre l'importance d'une approche intégrée couvrant à la fois la sécurité des systèmes d'information et la cybersécurité.

2.1.3 Importance de la sécurité de l'information dans les organisations et la société en général.

L'information, désormais considérée comme l'atout le plus essentiel pour les individus, les organisations et les sociétés, est le fondement même de notre compétence dans divers domaines. Sa sécurité demeure la priorité ultime, car elle garantit notre capacité à exceller dans ce que nous entreprenons. Dans un monde où la technologie est intimement interconnectée avec chaque aspect de la vie quotidienne, toutes les données, qu'elles soient en ligne ou stockées dans des bases de données, se retrouvent exposées à des vulnérabilités croissantes. La sécurisation de l'information devient ainsi impérative, non seulement pour préserver notre compétence, mais également pour assurer la confidentialité, l'intégrité et la disponibilité des données cruciales qui sous-tendent nos activités numériques. C'est dans ce contexte complexe et évolutif que la sécurité de l'information s'impose comme un objectif central, indispensable pour naviguer efficacement dans l'ère interconnectée de la technologie. (Ironhack, 2023)

En 2021, le coût mondial du cybercrime s'élevait à 6 000 milliards de dollars américains. On prévoit qu'il atteindra 10 500 milliards de dollars d'ici 2025. La menace croissante du cybercrime nécessite une réponse sérieuse, mettant en avant l'importance cruciale d'une infrastructure de sécurité robuste. (Figaro, 2022)

Les individus, les gouvernements, les entreprises, les organisations à but non lucratif et les établissements éducatifs sont tous exposés aux risques d'attaques et de violations de données. Dans le futur, le nombre d'incidents devrait augmenter en raison de l'évolution des technologies numériques, de l'expansion du nombre d'appareils et d'utilisateurs, de la complexité croissante des chaînes logistiques mondiales, et de l'importance stratégique croissante des données dans l'économie numérique. Afin de minimiser le risque d'attaques et de garantir la sécurité des systèmes et des données, la mise en place d'une solide infrastructure de cybersécurité devient essentielle. (OneLogin, 2021).

2.1.4 La triade CIA

Le fil rouge de la sécurité des informations d'une entreprise est le modèle de confidentialité, d'intégrité et de disponibilité, également appelé triade CIA. Il fait référence à un modèle de sécurité de l'information qui permet de garantir que les données d'une organisation ou d'une structure professionnelle sont protégées. La confidentialité, l'intégrité et la disponibilité sont les trois piliers d'une infrastructure protégée efficacement en matière de cybersécurité. En effet, ils sont essentiels à tous les programmes de sécurité. (TechTarget, 2016)

Confidentialité

Selon Marotte (2022), la confidentialité fait référence à la protection des données sensibles. Elle garantit que seules les personnes autorisées peuvent y accéder. Elle nécessite des mesures telles que le cryptage, les mots de passe solides et la classification des utilisateurs. Le cryptage est essentiel pour les transactions bancaires en ligne.

Exemple concret : Utiliser le chiffrement pour sécuriser les données sensibles des clients lors des transactions en ligne.

En somme, la confidentialité est essentielle pour empêcher l'accès non autorisé aux informations, nécessitant des stratégies appropriées à la sensibilité des données et une sensibilisation continue des utilisateurs.

Intégrité

Éviter toute altération non autorisée est crucial, en particulier lorsque la confidentialité est compromise. Des systèmes de surveillance avancés sont nécessaires pour détecter les modifications non intentionnelles, qu'elles proviennent d'événements externes tels qu'une impulsion électromagnétique ou d'incidents internes tels que le plantage d'un serveur.

Par exemple, il convient de prévenir et de détecter les violations de l'intégrité telles que la modification des informations bancaires sur un formulaire de paiement ou l'installation d'un virus par un cybercriminel, qui compromettent la fiabilité d'un réseau. (Gastard, 2023)

Exemple concret : Implémenter des contrôles de version pour assurer que les données ne sont pas modifiées de manière non autorisée, comme un système de gestion de versions dans un environnement de développement logiciel.

Accessibilité

Également appelée disponibilité, dans le contexte de la sécurité de l'information, elle garantit que les utilisateurs autorisés peuvent accéder aux données de manière opportune. Cela exige une maintenance régulière du matériel, des réparations immédiates en cas de besoin, et la gestion d'un environnement opérationnel fonctionnel, minimisant les conflits logiciels.

Selon Gastard (2023), bien que la confidentialité et l'intégrité soient des priorités, il est essentiel que les dispositifs de cybersécurité n'entravent pas l'accès aux informations. Chaque employé doit pouvoir accéder au contenu, aux réseaux et aux périphériques nécessaires. Les obstacles potentiels à la disponibilité incluent les coupures de courant, les attaques par déni de service et les défaillances matérielles ou logicielles.

Exemple concret : Mettre en place des sauvegardes régulières et des plans de reprise après sinistre pour garantir l'accès aux données en cas de panne système.

La triade CIA est la base de la sécurité de l'information. Quand il y a violation de données ou lorsqu'un incident de sécurité se produit, c'est que l'un ou plusieurs des principes mentionnés ci-dessus sont compromis.

Cependant, la sécurité de l'information est trop souvent reléguée à un rôle réactif axé sur la réponse aux besoins organisationnels et aux défaillances. Les organisations qui intègrent la gestion des risques dans leur culture et adoptent des stratégies proactives en mettant en œuvre des politiques d'infosécurité et de cybersécurité peuvent éviter de compromettre leur réputation, de perdre leurs données précieuses et, en fin de compte, d'avoir un impact négatif sur leur activité. (Marotte, 2022)

2.1.5 Parkerian Hexad model

La triade CIA est importante, mais elle n'est pas sacrée, et de nombreux experts en sécurité informatique vous diront qu'elle ne couvre pas tout. Donn Parker a proposé en 1998 un modèle à six côtés qui a été baptisé plus tard l'Hexade Parkerienne, qui repose sur les principes suivants : confidentialité, possession ou contrôle, intégrité, authenticité, disponibilité, utilité

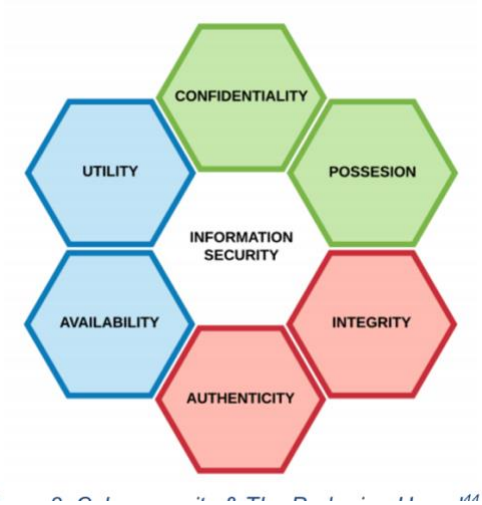


Figure 3: Parkerian hexad model

Source : Hartley, T. (2024, 2 avril). *The Parkerian Hexad : Elevating Information Security Beyond the CIA Triad.* The Profit - Inspiring Business In Hawke's Bay. Consulté le 17 avril 2024, à l'adresse https://www.theprofit.co.nz/govern-tom-hartley-pro-tech/

Le Parkerian Hexad model s'agit d'un modèle étendu de la triade CIA qui ajoute trois aspects supplémentaires : la possession, l'authenticité et l'utilité. Il offre une vision plus complète de la sécurité de l'information en incluant ces aspects supplémentaires.

Possession

La possession met l'accent sur le contrôle et la propriété de l'information. La possession garantit que les entités autorisées ont la propriété légitime et le contrôle sur les données ou les ressources, empêchant les entités non autorisées de revendiquer la possession. Les informations peuvent être confidentielles et avoir leur intégrité, mais entre de mauvaises mains, elles peuvent menacer ces deux caractéristiques.

Exemple concret : Assurer que les clés de chiffrement sont détenues uniquement par les administrateurs autorisés.

Authenticité

Ce principe aborde la fiabilité de l'information et l'assurance qu'elle est authentique et non falsifiée. L'authenticité garantit que les utilisateurs peuvent compter sur l'exactitude et l'origine de l'information. Par exemple, « Une méthode pour vérifier l'auteur d'un document manuscrit est de comparer les caractéristiques de l'écriture du document à un échantillon d'autres documents déjà vérifiés. Pour l'information électronique, une signature numérique pourrait être utilisée pour vérifier l'auteur d'un document numérique en utilisant la cryptographie à clé publique (elle pourrait également être utilisée pour vérifier l'intégrité du document). »

Exemple concret : Utiliser des signatures numériques pour vérifier l'origine et l'intégrité des documents électroniques.

Utilité

C'est une autre extension introduite par l'Hexad Parkerian, mettant l'accent sur l'utilité de l'information. L'utilité implique de garantir que l'information serve son but prévu et fournisse de la valeur aux utilisateurs autorisés tout en empêchant les abus.

Exemple concret : Garantir que les données cryptées peuvent être décryptées et utilisées par les utilisateurs autorisés.

En incorporant la possession, l'authenticité et l'utilité, l'Hexad Parkerian fournit une compréhension plus claire de la manière de traiter divers aspects de la sécurité de l'information, de la propriété, de la fiabilité et de l'utilisabilité. L'objectif ici de faire comprendre que la sécurité de l'information évolue et que les cadres également, il n'existe pas un seul et unique modèle universel sur la sécurité de l'information. Il y'en a qui sont plus connus que d'autres, mais les entreprises ne sont pas limitées. (Hartley et al., 2024)

2.2 Cybermenaces

Les cybermenaces constituent un défi majeur pour les organisations, et la directive NIS 2 vise à renforcer leur résilience face à ces menaces. Cette section se concentre sur les menaces les plus pertinentes pour la directive NIS 2 : les ransomware, le phishing, et les attaques DDoS.

La cybermenace englobe diverses formes de dommages potentiels visant les systèmes, les réseaux et les actifs numériques. Ces menaces peuvent perturber, désactiver, détruire ou accéder illégalement à ces systèmes, entraînant des conséquences telles que des violations de données, des pertes financières et des opérations compromises. L'ENISA définit les cybermenaces au sens large, en tenant compte non seulement des aspects techniques, mais aussi de l'intention et des capacités des acteurs de la menace, et en couvrant une série d'activités malveillantes telles que les ransomwares, les logiciels malveillants, l'hameçonnage et les attaques contre les infrastructures critiques. L'organisation souligne également l'importance d'une analyse et d'un rapport continus pour comprendre et atténuer ces menaces (European Union Agency for Cybersecurity, 2023)

Les cybermenaces et les attaques sont devenues plus fréquentes, plus sophistiquées et plus graves au cours des dernières années, avec des conséquences allant de l'atteinte à la réputation et aux finances jusqu'à la compromission d'opérations critiques.

Selon un rapport fait par Aon (2023), sur la résilience cybernétique, plus de la moitié des cyberévénements seront causés par des facteurs humains d'ici à 2025. Un autre rapport datant de 2023 fait état d'un élément humain dans 74 % de toutes les violations - de la simple erreur humaine et de l'ingénierie sociale à l'abus de privilèges et au vol d'informations d'identification.

IBM Security a publié en juillet 2023 son rapport annuel sur le coût d'une violation de données, montrant que le coût moyen mondial d'une violation de données a atteint 4,45 millions de dollars en 2023 - un record historique pour le rapport et une augmentation de 15 % au cours des trois dernières années. Les coûts de détection et d'escalade ont bondi de 42 % au cours de cette même période, ce qui représente la part la plus élevée des coûts de violation, et indique une évolution vers des travaux d'investigation plus complexes sur les violations.

Deux grandes tendances ont dominé le contexte européen en matière de cybermenaces : la montée de l'hacktivisme (se traduisant la plupart du temps par des opérations DDoS) et la croissance incessante d'attaques par rançongiciels (ransomware). L'hacktivisme (lié principalement aux tensions géopolitiques) a connu une expansion significative en 2023. De nouveaux groupes ont fait leur apparition, chacun apportant des tactiques et des cibles spécifiques, ce qui complexifie considérablement la tâche des professionnels de la cybersécurité dans le monde entier. Leurs actions, motivées par des raisons idéologiques diverses, ont conduit à un besoin accru de mesures de sécurité robustes dans tous les secteurs. (CCB, 2024-a)

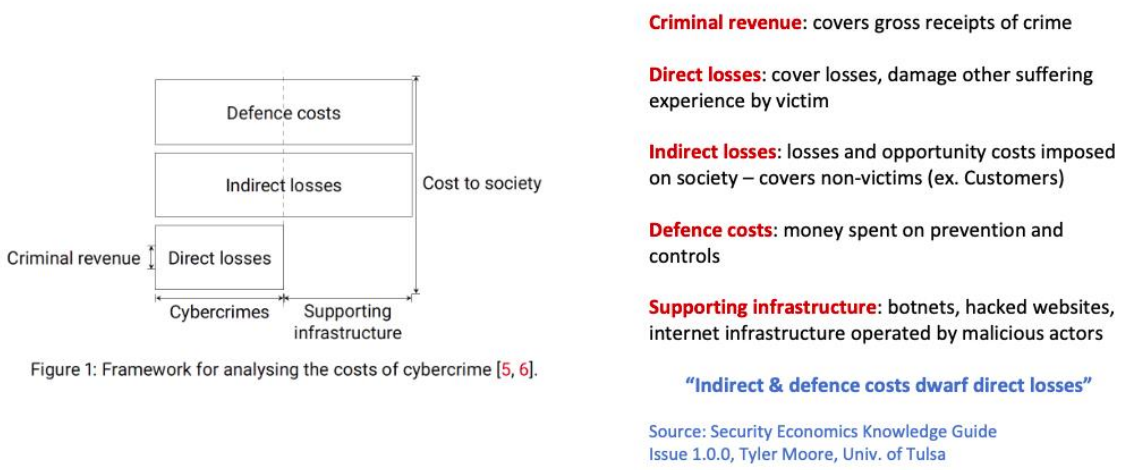


Figure 4: Le coût du cybercrime
Source : Moore, T. (2024, janvier). *Security Economics Knowledge Guide Issue 1.0.0*. Université de Tulsa. Consulté le 17 avril 2024, à l'adresse https://www.cybok.org/media/downloads/Security_Economics_KG_v1.0.0.pdf

La figure 4 présentée offre un aperçu éloquent de la disproportion entre les revenus tirés des cybercrimes et l'ampleur des coûts supportés par la société. Bien que les gains financiers des cybercriminels puissent sembler significatifs à première vue, ils sont en réalité minimes comparés aux pertes directes subies par les entreprises ciblées. Ces pertes directes, cependant, ne représentent que la pointe de l'iceberg. Le modèle met en lumière la véritable étendue des coûts induits par le cybercrime, qui va bien au-delà des sommes extorquées ou dérobées.

Les coûts indirects, qui incluent des éléments tels que la perte de productivité, la perturbation des opérations commerciales, et l'impact sur les clients, souvent non quantifiables immédiatement, contribuent à une charge économique considérablement plus lourde. De plus, les coûts de défense, constitués des investissements en sécurité informatique et des mesures préventives, représentent une part significative des dépenses, dépassant de loin les pertes directes. Ces coûts reflètent les sommes investies pour éviter ou minimiser les attaques futures, illustrant que le combat contre le cybercrime nécessite des ressources conséquentes.

L'ensemble de ces coûts à la société souligne une réalité frappante : les cyberattaques ont des ramifications financières qui s'étendent bien au-delà de l'acte illégitime initial, affectant une multitude de vecteurs économiques et démontrant que la portée des cybercrimes transcende largement les intentions et actions directes des cybercriminels.

Ce fut le cas de la British Library qui a subi une cyberattaque importante en octobre 2023 perpétrée par le groupe Rhysida spécialisé dans les ransomwares. Cette attaque a non seulement représenté une grave faille de sécurité, mais a également engendré de lourdes conséquences financières. Les méthodes d'attaque comprenaient le phishing, le spear-phishing et des attaques par force brute, facilitées par l'exploitation de données d'identification de tiers et par l'absence d'authentification multifacteurs. Les assaillants ont réussi à exfiltrer environ 600 Go de données, y compris des informations personnelles d'utilisateurs et de personnel de la bibliothèque, et ont causé des dommages importants à l'infrastructure de celle-ci. Les cybercriminelles exigeaient une rançon de 20 bitcoins équivalents à 596 000 livres à ce moment, afin de restaurer les services et leur rendre leurs données volées.

L'impact financier de l'attaque était considérable, avec des coûts de récupération estimés entre 6 et 7 millions de livres sterling, obligeant ainsi la British Library à envisager de dépenser près de 40 % de ses réserves financières. Suite à cela, la bibliothèque a entrepris un programme de "Reconstruction et Renouvellement" pour améliorer sa capacité à répondre à de tels incidents à l'avenir, avec un changement notable vers les technologies cloud. (France, 2024)

L'incident a mis en évidence plusieurs leçons importantes pour d'autres organisations, y compris la vulnérabilité inhérente aux infrastructures informatiques complexes et obsolètes, l'importance d'une protection robuste des points de terminaison et la nécessité d'une surveillance 24h/24 et 7j/7 pour lutter contre de telles menaces cybernétiques. Le système complexe de la bibliothèque, comprenant de nombreux systèmes désuets, a entravé la conformité aux normes de sécurité et a aggravé la gravité de l'impact de l'attaque.

La cyberattaque a eu un impact étendu, entraînant des perturbations opérationnelles telles que le retard des paiements du droit de prêt public, la suspension des programmes de bourses, et la mise hors ligne du catalogue en ligne de la bibliothèque ainsi que de la collection EThOS de thèses de doctorat britanniques pendant une période prolongée. Elle a également souligné la menace croissante des attaques par ransomware contre des institutions de toutes tailles et l'importance d'être préparé à de tels événements. (Stockley, 2024)

2.2.1 Le ransomware

J’ai déjà cité le ransomware qui est un logiciel malveillant, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur l’ordinateur et demande une rançon en échange de la clé permettant de les déchiffrer. Bien souvent, le ransomware s’infiltre sous la forme d’un ver informatique ou malware, à travers un fichier téléchargé ou reçu par email et chiffre les données et fichiers de la victime. La finalité est d‘extorquer une somme d’argent.

L’attaque par ransomware est restée l’activité cybercriminelle la plus importante affectant les organisations, y compris les infrastructures critiques, en Europe et aux États-Unis. Les opérateurs de ransomware ont principalement ciblé les secteurs suivants : l’industrie, les logiciels et les technologies de l’information (IT), les soins de santé, l’éducation, les services commerciaux et de conseil, le droit, la finance et le secteur bancaire. Depuis le début de la guerre en Ukraine, nous avons observé une augmentation des attaques par ransomware contre les municipalités et les institutions du secteur public dans les pays européens, y compris la Belgique. (CCB-b, 2024)

Dans près de deux tiers des cas, un seul jour suffit aux pirates pour perpétrer leurs méfaits. (Filippone, 2023). Donc malgré la multiplication des moyens mise en œuvre par les entreprises, pour détecter l’infection le plus rapidement possible, les cyberattaquants eux redoublent d'efforts pour réduire la période entre l'accès initial à un système cible et le moment où le ransomware est activé dans les entrailles d'un système informatique visé.

Selon une étude faite par MARSH McClennan (2022), sur les cyberattaques, ils ont analysé que les extorsions – principalement des ransomwares - représentaient la part la plus importante avec 38 %. Ce chiffre est plus élevé que les trois causes principales suivantes combinées, à savoir les violations de données (17 %), la cybercriminalité (10 %) et les enquêtes réglementaires (9 %). (Figure 5)

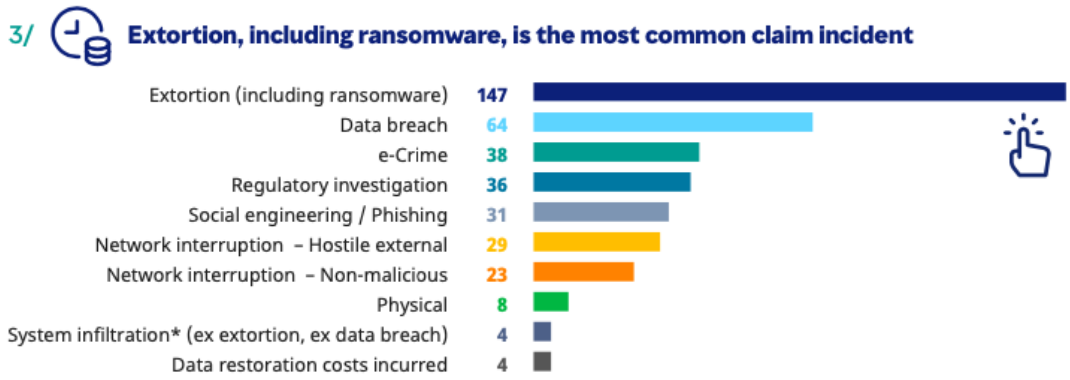


Figure 5: Les incidents les plus communs 2022

Source : Marsh. (2022, octobre). *The Changing Face of Cyber Claims 2022*. Consulté le 29 novembre 2023, à l'adresse https://www.marsh.com/fr/fr/services/cyber-risk/insights/the-changing-face-of-cyber-claims-2022.html

Le coût du silence - Les victimes de ransomware dans une étude faite par IBM qui ont fait appel aux autorités ont économisé 470 000 dollars en coûts moyens de violation par rapport à celles qui ont choisi de ne pas y faire appel. Malgré ces économies potentielles, 37 % des victimes de ransomware étudiées n'ont pas fait appel aux autorités lors d'une attaque par ransomware. Ces entreprises hésitent encore à faire appel aux autorités lors d'une attaque par ransomware, car elles pensent que cela ne fera que compliquer la situation. Alors qu'au contraire cela ne fait qu'allonger de 33 jours en moyenne les cycles de vie des violations.
De plus, près de la moitié (47 %) des victimes de ransomware étudiées auraient payé la rançon. Il est clair que les organisations devraient abandonner ces idées fausses sur les ransomwares. Le fait de payer une rançon et d'éviter les autorités ne peut qu'augmenter les coûts de l'incident et ralentir la réponse. (IBM France News Room, 2023.).

D'après le dernier rapport de l'éditeur Flare, les attaques de ransomware impliquant une extorsion de données ont connu une hausse de 112% par rapport à l'année précédente. Cette escalade s'explique en grande partie par la montée en puissance des cybercriminels qui se regroupent en collectifs de plus en plus structurés, tels que LockBit, AlphVM, CLOP ou encore BianLian.

En 2017, des multinationales telles que Saint-Gobain, Reckitt ou Mondelez ont été touchées par une cyberattaque massive impliquant les virus Petya et NotPetya. Les entreprises ont signalé des milliers d'ordinateurs bloqués, entraînant des perturbations majeures dans leurs opérations. Chez certaines entreprises, jusqu'à 80% des PC étaient hors service, entraînant des périodes prolongées de chômage technique pour les employés. Les entreprises ont également subi des pertes économiques importantes, avec des prévisions de réduction du chiffre d'affaires et des coûts supplémentaires liés à la gestion de la crise. Bien que la situation se soit améliorée dans certaines entreprises avec le rétablissement partiel des systèmes informatiques, les effets de la cyberattaque ont été ressentis pendant plusieurs semaines, voire quelques mois, après l'incident initial. (Godart, 2017)

La plus grosse attaque impliquant le virus NotPetya reste l'entreprise Maersk. L'entreprise Maersk a subi une cyberattaque dévastatrice en juin 2017 due à ce ransomware. L'attaque a été orchestrée par

des pirates informatiques soupçonnés d'être soutenus par le Kremlin, et a exploité les mécanismes de mise à jour d'un logiciel de comptabilité populaire en Ukraine, M.E.Doc. Cela a permis de propager le malware dans l'ensemble du réseau de Maersk qui est une des plus grandes entreprises du Danemark avec des entités à travers le monde.

L'impact de l'attaque sur l'entreprise a été immédiat et sévère. Le réseau de Maersk a été paralysé en seulement sept minutes, et la plupart des dommages ont été infligés dans l'heure qui a suivi. La restauration complète du système Active Directory de l'entreprise a pris neuf jours, un délai jugé inacceptable puisque l'objectif était de 24 heures.

Une coupure de courant à Lagos, au Nigeria, a par chance permis de sauver une copie de sauvegarde de l'Active Directory de Maersk, ce qui a été crucial pour la récupération de leurs systèmes. Malgré les défis liés à l'infrastructure de réseau publique limitée en Afrique de l'Ouest et l'absence de visa britannique pour le personnel local, l'entreprise a pu organiser le transfert de ces données vitales vers le centre de récupération en Grande-Bretagne.

L'incident a nécessité un effort mondial, avec des centaines d'employés travaillant sans relâche pour reconstruire le réseau. Pratiquement tous les ordinateurs portables de l'entreprise, près de 50 000, et le réseau de téléphones VoIP ont été détruits. Une réplique des ordinateurs et des serveurs a été rapidement organisée, y compris par l'achat d'ordinateurs dans les magasins de détail pour répondre à l'urgence. (Capano, 2023)

Au-delà de l'impact technique, cette attaque a eu des conséquences financières majeures. Maersk a estimé les coûts directs de NotPetya entre 250 et 300 millions de dollars, mais certains estiment que ces chiffres pourraient être bien en dessous de la réalité. L'incident a également eu un impact significatif sur les partenaires de l'entreprise et sur l'ensemble de la chaîne d'approvisionnement mondiale, accumulant des pertes se chiffrant en milliards de dollars.

Cette expérience a été une sonnette d'alarme coûteuse pour Maersk et le secteur en général. Elle a mis en lumière la nécessité d'une hygiène cybernétique et d'une défense robuste face aux menaces croissantes de la cyberguerre (Bannister, 2019).

Pour remédier à cela et répondre à une attaque de ransomware, plusieurs mesures peuvent être mises en place. Par exemple, le Centre pour la Cybersécurité Belgique, un service fédéral belge, a rédigé un guide qu'il met à disposition des organisations pour réagir en cas d'attaque par ransomware. Chaque organisation doit partir du principe que, tôt ou tard, elle sera confrontée à une attaque par ransomware ou autres. La principale question est de savoir quand. On peut retrouver des étapes comme le fait d'isoler les appareils affectés, mettre en place une équipe de gestion de crise, mettre en œuvre des mesures d'atténuation … (CCB, 2022)

2.2.2 Le phishing

Le phishing ou l'hameçonnage est également une de ces menaces émergentes, c'est un cybercrime qui consiste à utiliser de faux mails, sites Web et messages textes incitant la victime à révéler des informations personnelles et corporatives confidentielles : données de carte de crédit, numéro de

téléphone, adresse postale, informations sur une entreprise, etc. Ces informations sont ensuite utilisées par les criminels pour effectuer un vol d'identité et commettre une fraude. (Terranova Security, 2022)

Le phishing est resté l'un des principaux vecteurs d'attaque utilisés par les acteurs malveillants pour installer des logiciels malveillants dans un système ciblé, mais aussi l'un des types d'attaques les plus utilisés pour voler des données, telles que des informations personnelles et des données d'identification. Ces données sensibles seront ensuite exploitées pour mener des activités de cyberfraude. Les attaques par phishing s'appuient largement sur des techniques d'ingénierie sociale qui reposent sur l'erreur humaine plutôt que sur des vulnérabilités techniques et représentent un risque à la fois pour les organisations belges et pour les particuliers. (CCB, 2024-a)

Elle évolue et devient plus trompeuse en utilisant des tactiques d'ingénierie sociale plus élaborées pour tromper les victimes. Les e-mails de phishing peuvent sembler plus authentiques et persuasifs. En 1 an, le nombre d'attaques de phishing a augmenté de 47,2%. (Orange Corporate, s. d.).

Le phishing s'est d'abord développé à travers l'envoi de courriers électroniques frauduleux. En cliquant sur le lien contenu dans le mail, la victime est redirigée vers un faux site web. Mais les techniques d'hameçonnage évoluent : envoi de SMS (on parle de « smishing »), faux appels téléphoniques (« vishing ») … Désormais, les pirates perfectionnent leurs attaques avec l'IA qui leur permet de rendre leurs messages plus réalistes ou même d'usurper la voix de personnes de confiance.

En Belgique, les cybercriminels emploient souvent des leurres liés aux préoccupations courantes des citoyens, comme les notifications bancaires ou les services postaux, pour mener des attaques de phishing. Ces stratagèmes sont parfois convaincants, mais beaucoup peuvent être identifiés par des signes révélateurs. Récemment, les sujets ont évolué pour inclure des thèmes comme les subventions énergétiques et les contributions fiscales, tandis que les mentions liées au COVID-19 diminuent. Les campagnes visent principalement à dérober des informations, avec des malwares comme Agent Tesla et Loki password stealer parmi les plus répandus. (CCB, 2024-a).

Top 10 des familles de malware

Famille de malware	Total
agent tesla	545
xloader	124
remcos	68
snake keylogger	57
loki password stealer (pws)	46
cloudeye	41
blustealer	40
dbatloader	29
upatre	25
ave maria	22

Figure 6: Top 10 des familles de malware
Source : CCB. (2024-a, 11 janvier). *Projets et cybermenaces : CCB rapport 2023*. Centre Pour la Cybersécurité Belgique. https://ccb.belgium.be/fr/actualit%C3%A9/projets-et-cybermenaces-ccb-rapport-2023

2.2.3 DDoS

Une attaque en déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service. Ce type d'attaque peut être d'une grande gravité pour l'organisation qui en est victime. Durant l'attaque, le site ou service n'est plus utilisable, au moins temporairement, ou difficilement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité.
L'attaque est souvent visible publiquement, voire médiatiquement, et laisse à penser que l'attaquant aurait pu prendre le contrôle du serveur, donc potentiellement accéder à toutes ses données, y compris les plus sensibles (données personnelles, bancaires, commerciales…) : ce qui porte directement atteinte à l'image et donc la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires…

Le but est de rendre un service indisponible. Le cybercriminel agit pour des motivations politiques, idéologiques, par goût du challenge, chantage, vengeance, ou pour des raisons économiques (concurrence). Cette attaque peut être utilisée pour faire diversion d'une autre attaque visant à voler des données sensibles de sa cible. (Cybermalveillance.gouv.fr, 2019)

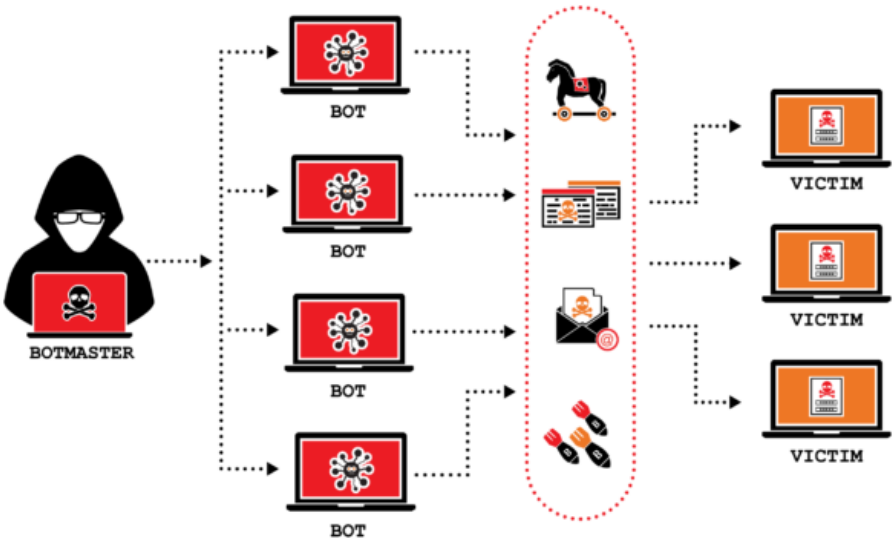


Figure 7: Représentation d'une attaque DDOS
Source : Thompson, A. (2021, 22 avril). *What Is a DDoS Attack ?*. Hashed Out By The SSL StoreTM. Consulté le 20 avril 2024, à l'adresse https://www.thesslstore.com/blog/what-is-a-ddos-attack/

En février 2018, GitHub a fait face à une attaque DDoS monumentale qui est devenue un événement marquant dans l'histoire de la cybersécurité.
GitHub, la plateforme de développement logiciel très fréquentée, a vu son fonctionnement interrompu à cause d'une attaque par déni de service distribué (DDoS) d'une ampleur sans précédent. Cette attaque a vu le volume du trafic entrant atteindre 1.35 téraoctet par seconde (Tb/s), ce qui a établi un nouveau record pour le plus grand assaut de ce type à l'époque.
Contrairement à d'autres attaques DDoS majeures qui avaient tendance à utiliser des réseaux de machines infectées (botnets), celle-ci a été menée en exploitant des serveurs de cache de base de données Memcached qui n'avaient pas été correctement sécurisés. Ces serveurs sont généralement utilisés pour améliorer les performances des applications web, mais ici, ils ont été détournés pour fonctionner comme des amplificateurs de trafic. (Kallenborn, 2018)

L'attaque a été initiée en falsifiant l'adresse IP de GitHub, envoyant ensuite de multiples petites requêtes aux serveurs Memcached. Les serveurs ont répondu par des quantités de données disproportionnées à cause d'une caractéristique d'amplification du protocole Memcached. L'effet net était que pour chaque requête envoyée, les réponses étaient beaucoup plus volumineuses, inondant ainsi GitHub de trafic.
Dès le début de l'attaque, GitHub a fait appel à Akamai, un service de protection contre les DDoS, qui a été en mesure de mitiger l'attaque en redirigeant le trafic malveillant. Environ 10 minutes après le début, GitHub était déjà en train de contrôler la situation, et après environ 20 minutes, l'attaque avait été complètement arrêtée. (Foltýn, 2018)

Ce cas a mis en lumière l'importance d'une préparation et d'une réaction rapides aux attaques DDoS, ainsi que le risque représenté par les serveurs et services internet mal configurés qui peuvent être exploités par des acteurs malveillants. Il a également souligné l'importance pour les entreprises de disposer de mesures de protection DDoS adéquates pour protéger leurs services en ligne contre de telles perturbations.

2.2.4 Tableau de synthèse

Dans le cadre de l'analyse des menaces cybernétiques, il est essentiel de disposer d'une compréhension claire et structurée des différentes formes d'attaques ainsi que de leurs spécificités. Le tableau suivant (Tableau 1) présente une synthèse comparative des 3 menaces présentées précédemment. Elles sont les plus prévalentes dans le cyberespace actuel : le ransomware, le phishing et DDoS. Chaque colonne distille les caractéristiques, méthodes d'attaque, impacts, et réponses associées à ces cybermenaces. Cette représentation permet non seulement d'appréhender les enjeux liés à chaque type de menace, mais offre également un aperçu direct des différences et similitudes dans leur approche, leur portée, et les défis qu'elles posent aux individus et aux organisations.

Cyber Menaces	**Ransomware**	**Phishing**	**DDoS**
Nature de la menace	Logiciel malveillant qui chiffre et bloque les fichiers	Cybercrime incitant à révéler des informations confidentielles	Attaque visant à rendre un service en ligne indisponible en le surchargeant de trafic
Méthode d'infection	Fichier téléchargé ou reçu par e-mail	Faux mails, sites Web, SMS (smishing), appels téléphoniques (vishing)	Surcharge de trafic provenant de multiples sources
Délai d'action	Une journée pour perpétrer l'attaque	Varie selon la réaction de la victime	Peut varier de quelques minutes à plusieurs jours
Taux d'incidence	38% des cyberattaques	Attaques fréquentes, 47,2% d'augmentation en un an	Fréquent, constitue une proportion significative des incidents de cybersécurité
Exemples notables	BlackCat, Black Basta, Royal	Agent Tesla, Loki password stealer	
Leçons apprises	L'importance de sauvegardes régulières et d'un plan de réponse aux incidents.	La nécessité d'une vigilance constante et d'une sensibilisation des employés.	Les attaques DDoS peuvent paralyser les opérations et nécessitent une préparation robuste.
Mesure de prévention	Mise en place de systèmes de détection précoce, formation des employés et utilisation de l'authentification multifactorielle.	Programmes de formation continue et mise en place de filtres anti-phishing robustes.	Utilisation de services de protection DDoS, surveillance continue du trafic réseau et préparation de plans de réponse aux incidents.
Incidents majeurs	Attaque de Petya/NotPetya en 2017, grandes entreprises affectées	Campagnes d'hameçonnage autour des préoccupations courantes	Attaque contre GitHub en 2018, une des plus importantes en termes de bande passante

Tableau 1: Tableau récapitulatif des cybermenaces les plus courantes.

D’autres types de menace tout aussi sophistiquée existent, je ne vais pas les citer, mais certaines ont été reprises dans le graphique ci-dessous. (*Figure 8*)

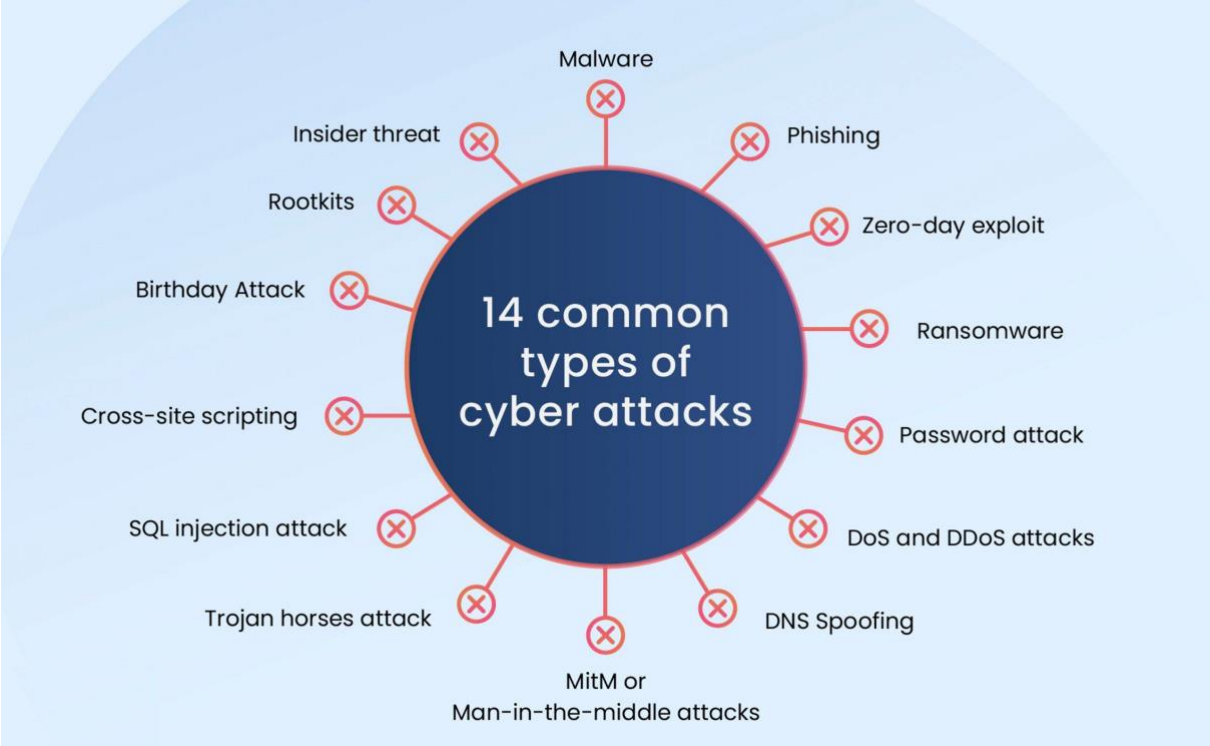


Figure 8: Graphique des menaces informatiques
Source : Yves. (2023, 12 juillet). *14 types de cyberattaques les plus courants (et comment les prévenir).* Inovency. Consulté le 13 mars 2024, à l’adresse https://inovency.fr/cybersecurite/cyberattaques-types-prevenir/

2.3 Technologies et risques associés

2.3.1 Enjeux

Une époque où notre société devient de plus en plus dépendante des technologies numériques, les frontières entre les réalités physiques et virtuelles deviennent de plus en plus floues. Dans ce monde sans frontières, la menace des cyberattaques est constante et imprévisible. Dans ce contexte, la technologie est à la fois une malédiction et une bénédiction. Elle offre de nombreux avantages, mais nous ne devons pas lui faire confiance aveuglément.

Il est à noter que la capacité d'adaptation des entreprises est souvent plus lente que le rythme de développement de ces nouvelles technologies. Selon une étude menée par le cabinet de consultance KPMG, 35% des entreprises citent la gestion des risques comme barrière principale à la mise en place de ces technologies. Donc les entreprises ont une certaine réticence quant au fait de passer le cap et investir dans une nouvelle solution innovante. (KPMG, 2020).

Selon Roy (2022), les technologies et systèmes numériques actuels présentent des opportunités et défis significatifs pour la sécurité des entreprises. Les avancées telles que l'intelligence artificielle, la

blockchain, l'internet des objets et le Big Data redéfinissent la sécurité, augmentant les risques liés à la sécurité des réseaux, des informations, des données et la cybersécurité. La capacité à s'adapter et à adopter une vision holistique est cruciale pour faire face à l'évolution des menaces dans le contexte mondial. L'environnement technologique en évolution rapide met au défi les mesures d'atténuation des risques actuelles, soulignant l'importance d'une intervention immédiate pour maintenir l'intégrité et la confiance dans les technologies futures. Les implications de la stratégie de cybersécurité sur la sûreté et la sécurité humaines requièrent une meilleure compréhension du paysage des cybermenaces et une coordination des réponses aux défis futurs.

Cinq défis majeurs émergent pour sécuriser l'écosystème numérique, incluant le déficit de compétences en cybersécurité, la fragmentation des approches techniques et politiques, l'adaptation insuffisante des capacités de sécurité opérationnelle, le sous-investissement dans la sécurité des technologies émergentes, et l'ambiguïté de la responsabilité. L'interaction entre ces défis nécessite une action collective pour établir un niveau de cybersécurité adéquat et une capacité à identifier et surveiller les risques dans l'ensemble de l'écosystème.

Un autre exemple du fait que le nombre de régulations et de mises en conformité augmente drastiquement est l'AI act, qui est une proposition législative de l'Union européenne destinée à encadrer le développement et l'utilisation de l'intelligence artificielle. C'est le premier cadre juridique exhaustif à l'échelle mondiale pour l'IA, visant à garantir la sécurité, la conformité aux droits fondamentaux et une certaine uniformité juridique pour les entreprises au sein des États membres. L'objectif est de favoriser la confiance dans les technologies d'IA en assurant leur transparence et leur responsabilité. De plus, l'initiative 'GenAI4EU' appuie les start-ups et les PME dans la création d'IA conforme aux valeurs de l'UE. Ces efforts visent à encourager l'innovation tout en assurant la fiabilité et les standards éthiques de l'IA dans divers secteurs et le secteur public. (Commission européenne, 2024).

2.3.2 Exemple de technologies

Diverses technologies émergent actuellement, et les entreprises s'efforcent de les intégrer et de les maîtriser (Roy, 2022), notamment :

1. **Intelligence Artificielle (IA)** : L'IA est devenue essentielle pour la détection proactive des cyberattaques et la protection des organisations en ligne. Elle offre un soutien avancé aux professionnels de la sécurité grâce à des capacités d'apprentissage et d'analyse qui permettent d'identifier et de contrer les menaces de manière efficace. Elle vise à créer des machines capables de simuler l'intelligence humaine. Dans le contexte de la cybersécurité, l'IA est utilisée pour automatiser des tâches complexes telles que la détection d'anomalies, l'analyse de comportement des utilisateurs et la réponse aux incidents.
    Machine Learning (ML), une sous-discipline de l'IA permet aux systèmes de s'améliorer avec l'expérience en apprenant à partir de données passées. Par exemple, les algorithmes de ML peuvent détecter des schémas de comportement suspects dans les journaux d'accès réseau. (David, 2021)
2. **Blockchain** : Cette technologie de registre distribué assure la sécurité et la transparence des transactions sur internet, réduisant les risques de violations de données, de cyberattaques, de vol

d'identité, et de fraude. La blockchain garantit la confidentialité et l'intégrité des données à travers son système décentralisé.

3. **Internet des Objets (IoT)** : Avec la prolifération des appareils connectés, la sécurité de l'IoT devient une préoccupation majeure. Bien que les risques soient élevés, des mesures sont mises en place pour protéger les données échangées entre ces appareils et prévenir les cyberattaques. Elle se réfère aux objets connectés à internet, tels que les capteurs, les caméras de sécurité, les thermostats intelligents, etc. Ces appareils collectent et échangent des données. Ces appareils peuvent être vulnérables aux attaques. Des mesures telles que l'authentification forte, le chiffrement des données et la segmentation du réseau sont nécessaires pour protéger l'IoT.
4. **Big Data** : Le Big Data est un outil à double tranchant en cybersécurité. Il permet aux analystes de détecter les anomalies et les menaces potentielles en analysant de vastes volumes de données. Cette capacité à traiter et à analyser des informations complexes en temps réel est cruciale pour la détection rapide des cybermenaces. Cependant, le Big Data présente également des défis, notamment la gestion de la confidentialité des données et la capacité d'extraire des informations pertinentes parmi le bruit.

En conclusion, l'émergence rapide des technologies telles que l'intelligence artificielle, la blockchain, l'internet des objets et le Big Data offre des opportunités remarquables pour améliorer l'efficacité des entreprises. Cependant, ces avancées s'accompagnent de nouveaux défis en matière de cybersécurité. Il est crucial pour les entreprises de rester vigilantes, de s'adapter rapidement et d'adopter des approches holistiques pour sécuriser leur écosystème numérique dans un paysage technologique en constante évolution.

2.4 Émergence des réglementations

L'évolution du nombre de réglementations européennes en matière de cybersécurité, comme illustrée dans la figure ci-dessous (figure 9), témoigne d'une prise de conscience accrue et d'une réponse structurée aux enjeux numériques contemporains. Ce paysage réglementaire ne cesse de se densifier, la directive NIS 2 ne surgissant pas ex nihilo, mais s'inscrivant dans une vague progressive et réfléchie de législations. Elle s'articule avec des textes fondateurs tels que le RGPD, qui a marqué un tournant dans la protection des données personnelles, ou encore la directive Whistleblower, soulignant l'importance de la transparence et de la protection des lanceurs d'alerte. L'acte de résilience cybernétique et le Cybersecurity Act, avec ses certifications en cybersécurité, établissent des standards élevés pour les produits et services numériques, contribuant à renforcer la confiance des utilisateurs. La directive sur la résilience des entités critiques et le Digital Operational Resilience Act (DORA) pour le secteur financier sont des exemples de la manière dont l'UE adapte continuellement son cadre réglementaire pour répondre aux défis posés par l'intégration technologique dans des domaines essentiels. Ainsi, la directive NIS 2 s'inscrit comme le dernier maillon d'une chaîne de mesures visant à édifier une Europe numérique sûre et sécurisée, reflétant des années d'expérience réglementaire et de maturation stratégique.

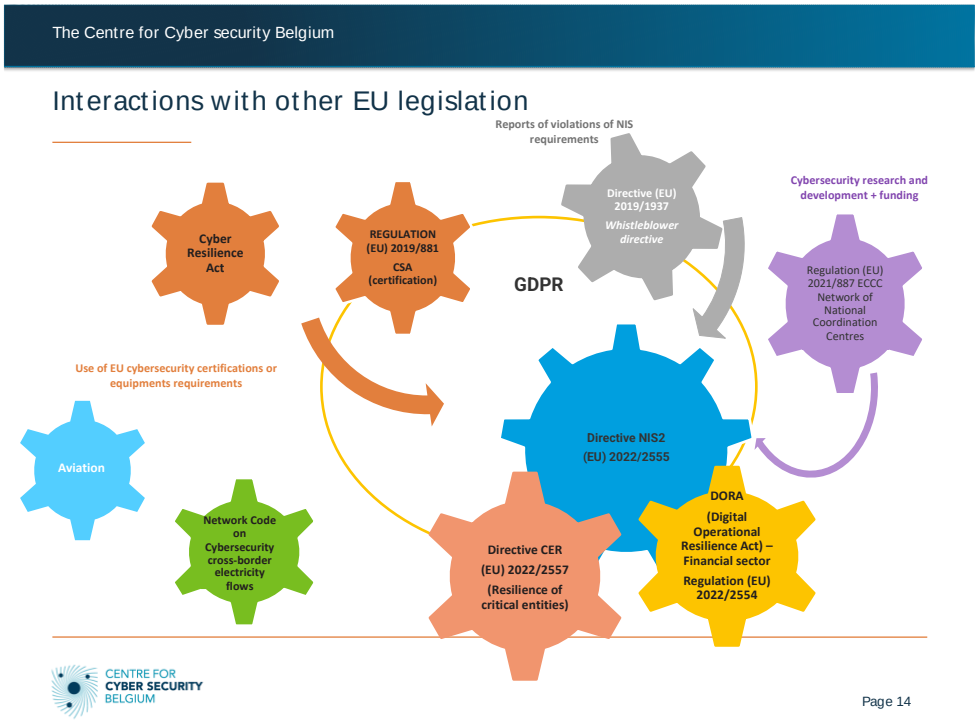


Figure 9: L'interaction entre les législations européennes
Source : CCB. (2023, juin) *NIS 2 in BE* [Présentation Power Point]. CCB

L'ensemble de ces mesures, renforcé par la création de réseaux de coordination nationaux, révèle une stratégie intégrée et dynamique, anticipant et façonnant la résilience face aux cybermenaces de manière proactive au sein de l'Europe. Elle s'assure aussi à ce dont tous les citoyens et business peuvent bénéficier pleinement de services digitaux fiables.

2.4.1 Le RGPD

2.4.1.1 La définition du RGPD

Les entreprises doivent se conformer au règlement européen sur la protection des données (RGPD). Il est entré en application en 2018 et impacte toutes les entreprises opérant du traitement de données à caractère personnel sur des résidents européens.
Elle s'applique aux administration et entreprise qui gèrent des données personnelles et sert à encadrer la manière dont elles vont les utiliser.
Il poursuit plusieurs objectifs ambitieux, tels qu'uniformiser au niveau européen la réglementation sur la protection des données, responsabiliser davantage les entreprises en développant l'autocontrôle, etc. (CNIL, 2016).

Mais son objectif principal reste le fait d'assurer aux citoyens une relative sécurité des données personnelles qu'elles communiquent souvent aux entreprises sans en mesurer les enjeux (Ragheno, 2017). Le but est également de mettre une limite à la manière dont nos données sont exploitées.

2.4.1.2 Données personnelles

Pour les entreprises, elles doivent pouvoir prouver à n'importe quel moment que les données personnelles dont elle dispose ont été recueillies de façon légale, avec le consentement de l'utilisateur, qu'elle les garde bien sécurisées.
Une donnée à caractère personnel selon la Commission européenne est toute information se rapportant à une personne vivante identifiée ou identifiable. Différentes informations, dont le regroupement permet d'identifier une personne en particulier, constituent également des données à caractère personnel. (Commission européenne, s. d.-a)

Figure 10: Exemple de donnée personnelle couverte par le RGPD
Source : Bouche, T.-J. (2020, 27 janvier). *Donnée à caractère personnel : Qu'est ce que c'est ?*. DPO Expert. Consulté le 14 février 2024, à l'adresse https://dpoexpert.fr/donnee-a-caractere-personnel/

2.4.1.3 Les sanctions

Dans le contexte du Règlement Général sur la Protection des Données (RGPD), il est crucial de noter que les violations des obligations imposées au responsable de traitement et au sous-traitant peuvent entraîner de lourdes sanctions. Le règlement fournit différentes options aux autorités de protection des données en cas de non-respect des règles sur la protection des données :

- Possible violation : un **avertissement** peut être émis ;
- Violation : les sanctions comprennent un rappel à l'ordre, une interdiction temporaire ou définitive du traitement et une amende pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total de l'entreprise.

L'autorité doit s'assurer que les amendes imposées dans chaque cas d'espèce
sont effectives, proportionnées et dissuasives. (Commission européenne, s.d.-c)

2.4.1.4 Exemple de sanction possible

Une entreprise vend des articles ménagers en ligne. Grâce à son site internet, les clients peuvent acheter des appareils électroménagers, des tables, des chaises et d'autres articles domestiques en communiquant

leurs informations bancaires. Le site internet subit une attaque informatique et toutes les informations personnelles sont désormais à la disposition du pirate. Dans ce cas, le manque de mesures techniques appropriées mises en place par l'entreprise semble être la cause de cette perte de données.
Cet exemple partagé par la Commission européenne nous permet de mieux comprendre en quoi cela consiste et pourquoi il est important qu'une entreprise respecte les normes de conformité afin d'éviter les sanctions.

Différents facteurs seront donc pris en considération par l'autorité de contrôle avant de décider des mesures correctrices à adopter. Des facteurs tels que : la gravité des lacunes du système informatique, la durée de l'exposition de l'infrastructure informatique à ce risque, les tests menés dans le passé pour prévenir ce genre d'attaque, le nombre de clients dont les données ont été volées ou divulguées, le type de données à caractère personnel affecté (comme des données sensibles). Toutes ces considérations et d'autres seront prises en compte par l'autorité de contrôle.

Ce fut le cas pour META, la société mère de Facebook qui détient donc la plus grosse amende jamais donnée par rapport au GDPR. En mai 2023, ils ont été sanctionnés d'une amende de 1,2 milliard d'euros pour avoir transféré les données collectées auprès des utilisateurs de Facebook dans l'Union européenne aux États-Unis, en violation des lignes directrices du GDPR en matière de transfert international. (Komnenic, 2024)

2.4.1.5 Mise en application du RGPD

Il y a différentes étapes clés à suivre pour une entreprise afin de se mettre en conformité avec le RGPD. Tout d'abord désigner un pilote, un responsable de projet qu'on nommera DPO. Il sera l'acteur central du projet et veillera au respect de différente tâche. Ensuite, il faut cartographier les traitements de données personnelles. Sur cette base-là, l'entreprise va prioriser les actions à mener. Les données personnelles susceptibles d'engendrer des risques élevés doivent être gérées. La 5^{e} étape est la mise en place de procédures internes qui garantissent la prise en compte de la protection des données. Pour finir, tout cela doit être documenté pour prouver la conformité au Règlement. (Féraud-Courtin & Flambard, 2017)

Selon l'article 32 de ce règlement général, la protection des données personnelles nécessite de prendre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. (GDPR Info, 2016)

Une telle approche permet en effet une prise de décision objective et la détermination de mesures strictement nécessaires et adaptées au contexte. Il est cependant parfois difficile, lorsque l'on n'est pas familier de ces méthodes, de mettre en œuvre une telle démarche et de s'assurer que le minimum a bien été mis en œuvre. (CNIL, 2018)

C'est pour cela que les activités de l'entreprise sont souvent soumises à des exigences de conformité. Plusieurs organismes, dont le NIST (National Institute of Standards and Technology) et l'ISO (Organisation internationale de normalisation), ont ainsi établi des normes de gestion des risques pour aider les entreprises à se conformer à ces exigences et à garantir une gestion efficace des risques. (RedHat, 2019).

Elles vont leur offrir une sorte de guide à suivre afin de mettre en œuvre les bonnes pratiques de façon systémiques.
D'autres cadres de références liés à des recommandations dans les services IT comme ITIL, ou dans le contrôle et gouvernance comme COBIT, ou dans d'autres références connues dans la rédaction de cadre efficace dans le contrôle interne lié au risque par COSO, etc. seront aussi exploités dans le mémoire. Nous les traiterons plus tard dans le travail.

2.4.2 CSA

La Cybersecurity Act concerne la certification des produits, services et processus des Technologies de l'Information et de la Communication (TIC) (Ministry of Economic Affairs and Climate Policy, 2023). Au cours des dernières années, de nombreux pays ont adopté différentes méthodes de certification de leurs TIC. Toutefois, en raison du grand nombre de certifications disponibles et de leur manque d'uniformité, l'Union européenne a souhaité mettre en place un cadre de certification uniforme et reconnu internationalement. Ce cadre vise à garantir que les produits numériques respectent des normes de sécurité élevées, offrant ainsi une meilleure protection contre les cybermenaces. En unifiant les procédures de certification, l'UE cherche à simplifier le processus pour les entreprises et à renforcer la confiance des consommateurs dans les produits et services numériques.
En Belgique, l'entité responsable de la représentation de cette loi au niveau européen est le CCB. Son rôle consiste essentiellement à délivrer les certificats et à infliger des sanctions en cas de besoin (Cyber Security Coalition, 2021).

La création d'un cadre de certification unifié présente plusieurs avantages. Tout d'abord, cela facilite la compréhension des différentes certifications et fournit un langage commun dans l'ensemble de l'UE. Cela permet également de réduire la fragmentation du marché en harmonisant les exigences de sécurité à travers les pays membres. De plus, cela favorise la compétitivité des entreprises européennes sur le marché mondial en renforçant la confiance des consommateurs dans les produits numériques européens.

2.4.3 CRA

Cyber Security Resilience Act (CRA) cible un large éventail de produits grand public, notamment l'IoT, le cloud, les communications, les paiements, l'automobile, et bien d'autres encore. Les développeurs de produits seront tenus de protéger leurs systèmes et réseaux contre les menaces cybernétiques, et de signaler les incidents de sécurité significatifs. En d'autres termes ce texte porte sur les produits comprenant des éléments numériques permettant la transmission de données à un appareil ou à un réseau.

Ce règlement a vocation à promouvoir la confiance dans les technologies numériques en garantissant qu'elles répondent à des normes de sécurité rigoureuses ; les fabricants devront ainsi s'assurer que les objets connectés mis sur le marché respectent des obligations strictes. Les professionnels auront en cas d'incident une obligation déclarative impactant la sécurité des produits numériques mis sur le marché. (Glaser, 2024)

Le CRA a été créé comme moyen de résoudre deux problèmes principaux en matière de cybersécurité. Le premier concerne "le faible niveau de cybersécurité des produits comportant des éléments numériques, reflété par des vulnérabilités généralisées et la fourniture insuffisante et incohérente de mises à jour de sécurité pour y remédier." (European Cyber Resilience Act (CRA), 2022). Le deuxième

problème concerne la connaissance limitée des produits dotés d'une cybersécurité adéquate. Les objectifs de cette loi sont triples. Premièrement, elle a mis en place un ensemble de règles à respecter lors du lancement d'un produit comportant un élément numérique. Deuxièmement, elle a créé un cadre de cybersécurité avec des exigences à respecter en matière de maintenance, de conception, etc., d'un produit cybernétique. Enfin, elle garantit un devoir de diligence du produit pendant toute sa durée de vie (Commission européenne, 2020).

Dans l'ensemble, cette loi a été créée pour protéger les consommateurs, mais aussi les entreprises des dangers des produits numériques. Elle assure la sécurité de ces produits tout au long de leur cycle de vie et offre une sorte de garantie aux utilisateurs de ces produits. Il s'agit là d'une autre étape vers la résilience et la sécurité.

2.4.4 DORA

DORA, ou la Digital Operational Resilience Act, est une proposition de règlement de l'Union européenne visant à renforcer la résilience opérationnelle des entités du secteur financier face aux risques numériques, tels que les cyberattaques, les pannes technologiques et les incidents de sécurité. Elle est entrée en vigueur le 16 janvier 2023, étant noté que la date d'application du Règlement « DORA » est prévue le 17 janvier 2025, date butoir de transposition de la directive.

DORA vise à garantir que les prestataires de services financiers, telles que les banques, les compagnies d'assurances et autres instances des marchés financiers maintiennent des normes élevées de sécurité de leurs systèmes d'information et de gestion des risques opérationnels au regard des données et flux qu'elles enregistrent. (European Securities and Markets Authority, 2023).

Le règlement propose ainsi des mesures telles que l'obligation pour les prestataires de services financiers de mettre en œuvre des plans de continuité des activités et des tests de résistance aux cyberattaques.
De la même manière, ce règlement organise les relations contractuelles entre les prestataires tiers de services TIC et les entités financières
En outre, DORA prévoit des mécanismes de supervision renforcés, avec la création d'une autorité européenne dédiée chargée de superviser la conformité et d'imposer des sanctions en cas de non-respect des règles. La proposition prévoit des sanctions dissuasives en cas de non-respect des obligations établies, y compris des amendes financières importantes. (Glaser, 2024)

Le concept de résilience opérationnelle met ainsi l'accent sur la nécessité de faire évoluer l'approche de gestion des risques opérationnels, d'une approche centrée sur la prévention des risques et la limitation des pertes vers une approche plus large et proactive. Cette dernière part du principe que les incidents, même les moins probables, vont se produire et qu'il faut être prêt à les traiter et à assurer la continuité des activités et services critiques ou importants.

Ces concepts et principes mentionnés ici seront également repris dans le NIS 2. Cette volonté accrue de gestion des risques proactive et de mise en place des meilleures pratiques pour éviter tout type d'incident ainsi que pour y répondre de la meilleure des manières est une volonté qu'on retrouve dans ces différentes réglementations et directives.

2.4.5 Tableau de synthèse

Le tableau suivant présente une synthèse comparative de ces quatre réglementations clés, mettant en évidence leurs principaux objectifs, domaines d'application, sanctions en cas de non-conformité, et leur statut d'entrée en vigueur.

Règlement	Objectif Principal	Domaine d'Application	Sanctions en cas de Non-conformité	Entrée en Vigueur
RGPD	Protection des données personnelles et renforcement de la confidentialité en UE	Toutes les entreprises traitant des données personnelles des résidents de l'UE	Amendes jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial	2018
CSA	Établir un cadre de certification unifié pour les produits TIC en UE	Certification des produits, services et processus des TIC	Sanctions par l'autorité compétente en cas de non-respect des certifications	2019
CRA	Améliorer la cybersécurité des produits à éléments numériques et leur durée de vie	des produits grand public comprenant l'IoT, le cloud, les paiements, l'automobile, etc.	Obligations déclaratives et exigences de sécurité pour les fabricants	2022
DORA	Renforcer la résilience opérationnelle des entités financières face aux risques numériques	Prestataires de services financiers, banques, assurances, et autres entités financières	Sanctions financières significatives et renforcement de la supervision	2023 (Application prévue pour 2025)

Tableau 2 : Tableau récapitulatif des nouvelles réglementations et directives.

2.5 Gestion des risques

2.5.1 Définition

Selon la norme ISO 31000 : « Les organismes de toutes sortes sont confrontés à des facteurs et des influences internes et externes, de sorte qu'ils ignorent s'ils vont atteindre ou dépasser leurs objectifs et, si oui, à quel moment et dans quelle mesure. L'incidence de cette incertitude sur l'atteinte des objectifs d'un organisme constitue le risque. » (ISO, s. d.).

La gestion des risques quant à lui est un processus vital pour les entreprises, impliquant l'identification et l'évaluation des risques potentiels auxquels elles sont confrontées. L'objectif est de développer un plan robuste visant à protéger l'organisation contre les pertes financières, les atteintes à sa réputation, ou tout autre préjudice pour ses employés. Ces risques peuvent provenir de diverses sources, notamment les conditions du marché, les évolutions réglementaires, ou les menaces cybernétiques.

Catégories de risques auxquels l'entreprise fait face

Catégories de risques	*Nature du risque*
Risque financier (de change, opérationnel, de marché, de crédit, de taux d'intérêt)	Risque financier : changements dans le taux d'intérêt, le change, le crédit, la valeur de l'instrument financier et la liquidité. Risque opérationnel : défauts techniques, accidents, erreurs humaines, perte d'employés clés. Risque du marché : changements dans la concurrence, dans le nombre de produits vendus par client, perte de parts de marché.
Risque lié à la réglementation gouvernementale	Changement dans le contrôle, la réglementation, les législations nationales et internationales
Risque économique	Changements dans les facteurs macroéconomiques.
Risque de matières premières	Changements dans les prix des matières premières
Risque environnemental	Incidents dans l'environnement, lois et règlements environnementaux
Risque politique	Conduite des affaires dans un contexte international
Risque d'illiquidité	Les difficultés de faire face à ses engagements, à ses échéances
Risque de technologie	Changement rapide de technologie
Risque lié aux conditions climatiques	Conditions climatiques graves, défavorables à l'activité de l'entreprise
Risque fournisseur	Dépendance à l'égard de fournisseurs clés, fournisseurs peu sûrs
Risque lié au cycle	Tendance cyclique naturelle
Risque de saisonnalité	Modèles saisonniers
Risque de valeur de l'instrument financier	
Risque de distribution	Changements dans les canaux de distribution
Risque de ressources naturelles	Quantités insuffisantes de réserves, faible qualité des réserves.

Figure 11 : Gérer le risque à l'échelle de l'entreprise

Source : Ebondo Wa Mandzila, E., & Zéghal, D. (2009). *Management des risques de l'entreprise : Ne prenez pas le risque de ne pas le faire !* La Revue des Sciences de Gestion, (237-238), 5-14. https://www.cairn.info/revue-des-sciences-de-gestion-2009-3-page-5.htm

Une entreprise qui connaît ses risques développe une agilité propice à la résistance et au rebond. Des scénarios de crise et un plan de continuité permettent d'envisager les situations et de mettre en place des solutions de repli qui rendent l'organisation résiliente quand la crise surgit. Les stratégies de gestion des risques sont les tactiques mises en place pour traiter ces risques et comprendre leurs répercussions possibles. Elles sont intégrées dans un plan de gestion des risques, un processus documenté qui décrit les méthodes utilisées par une entreprise ou une équipe pour identifier et remédier aux risques émergents. En adoptant une approche proactive de la gestion des risques, une organisation peut réduire les chances que quelque chose se passe mal et minimiser les dommages. (SafetyCulture, 2024)

Un processus de gestion des risques implique :

- L'identification méthodique des risques entourant les activités de l'entreprise
- L'évaluation de la probabilité qu'un événement survienne
- La compréhension de la façon de répondre à ces événements
- La mise en place de systèmes afin de faire face aux conséquences
- La surveillance de l'efficacité des approches et contrôles en matière de gestion des risques

En conséquence, le processus de gestion des risques améliore la prise de décision. En effet, cela permet de mieux maîtriser les flux d'informations, d'obtenir une meilleure évaluation des risques et, ainsi, de gagner en agilité et en visibilité pour faire les bons choix. Elle permet également la planification et la priorisation, elle aide à allouer le capital et les ressources de façon plus efficace, permet d'anticiper ce qui pourrait mal tourner, de minimiser le nombre de feux à éteindre ou, dans le pire des cas, d'empêcher un désastre ou une grave perte financière, et améliore de façon importante la probabilité livrer le plan d'affaires en temps voulu et conformément au budget. (Info Entrepreneurs, 2023)

Ce processus de gestion des risques est une approche générale largement acceptée et utilisée dans de nombreuses organisations. Cependant, nous examinerons d'autres cadres de référence, où nous pourrons constater que des étapes supplémentaires sont souvent incluses pour fournir une structure plus détaillée et complète de la gestion des risques.

2.5.2 Importance de la gestion des risques

Pour replacer l'importance de la gestion des risques dans son contexte, il existe plusieurs exemples contemporains et résultats de recherche qui montrent l'impact préjudiciable des risques non gérés sur les entreprises.
Le monde connaît aujourd'hui une instabilité qui est difficilement lisible pour les entreprises. La tension est permanente et les sanctions peuvent prendre de multiples formes.
Les organisations doivent se préparer à affronter une série de crises, qu'elles soient d'ordre politique, économique, sanitaire ou climatique. Ces crises peuvent survenir de manière imprévisible et avoir des conséquences dévastatrices sur les entreprises. Par exemple, au cours des dernières années, outre la pandémie, les entreprises ont été confrontées à une augmentation des cyberattaques, à des événements climatiques extrêmes, au blocage du canal de Suez. Ces crises affaiblissent les organisations et ont un impact négatif sur leurs résultats financiers, leur capacité d'innovation et la confiance de leurs employés. (Bergé, 2021)

Selon l'étude menée par IBM Security, il y a des lacunes en matière de détection - seul un tiers des violations étudiées ont été détectées par l'équipe de sécurité de l'organisation, alors que 27 % ont été

divulguées par un pirate. Les violations de données divulguées par un pirate coûtent en moyenne près d'un million de dollars de plus que celles des organisations étudiées qui ont identifié elles-mêmes la violation.

Stéphanie Talaud, directrice IBM Security déclare : « Tout est une question de temps … Plus on met de temps à détecter une intrusion grave, plus l'impact est fort et coûteux, il faut donc mettre en œuvre de nouvelles approches ». Elle y rajoute : « Il n'est plus suffisant de réagir, il faut pouvoir prédire au mieux et anticiper pour agir plus vite, de manière proactive et les solutions d'IA et d'automatisation peuvent s'avérer être un atout majeur pour cela ».

L'évaluation du coût du risque dans une entreprise exige de trouver un équilibre entre le coût des mesures préventives et le coût des pertes potentielles dues aux risques non gérés. La gestion du risque se base sur ce que l'organisation est prête à accepter comme pertes en échange d'un investissement initial dans des mesures de protection. L'objectif est de parvenir à un point où le coût de la gestion proactive du risque est compensé par la réduction du risque de pertes significatives, aboutissant à une situation financièrement avantageuse sur le long terme. Cet équilibre est trouvé lorsque le coût des dispositifs de protection et l'impact des risques résiduels, ceux qui subsistent malgré les mesures prises, sont tous deux optimisés pour garantir la rentabilité. (Figure 12)

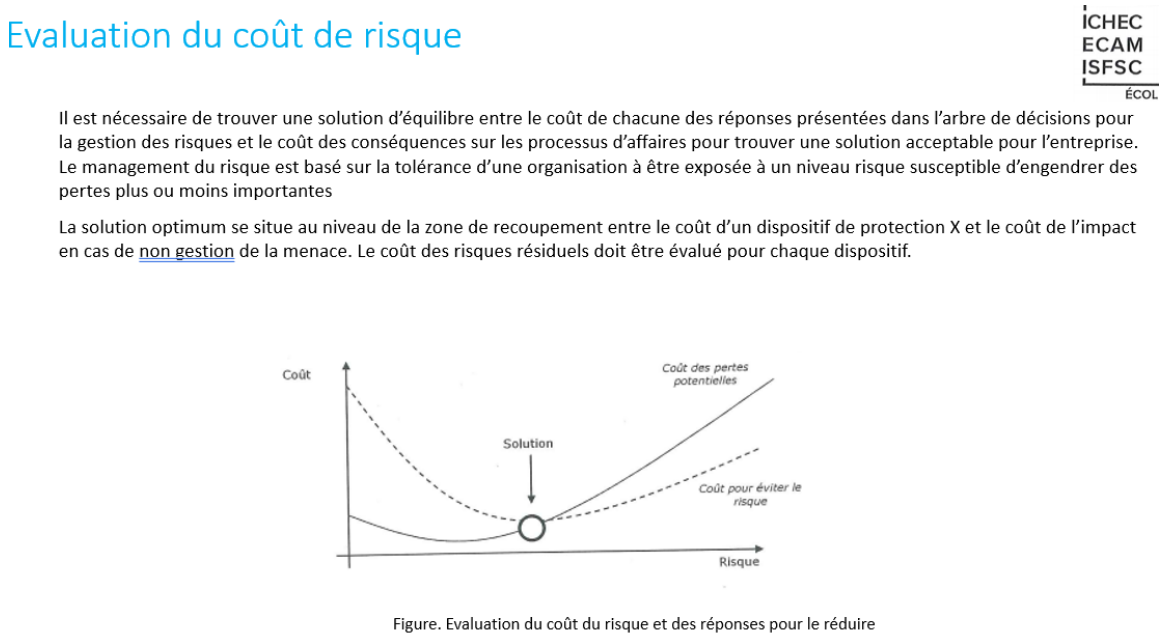


Figure 12: Évaluation du cout de risque
Source : Georgel. (2009). *Évaluation du cout de risque* [Présentation Power Point]. ICHEC.

Dans la théorie de la gestion des risques, il est primordial pour un décideur d'évaluer si un risque est acceptable en fonction des coûts associés. Ce processus commence par l'identification des menaces et l'évaluation de la vulnérabilité des ressources informatiques de l'organisation à ces menaces. Si une vulnérabilité existe, un risque est donc présent. Le décideur doit alors déterminer si le coût associé à la réduction de ce risque est justifié par rapport au gain potentiel. Si la réduction du risque s'avère coûteuse, une estimation des pertes potentielles est réalisée pour définir si elles dépassent le seuil d'acceptabilité de l'entreprise. En cas de dépassement, un audit IT est recommandé pour approfondir l'analyse et orienter les décisions concernant la gestion du risque. (Figure 13)

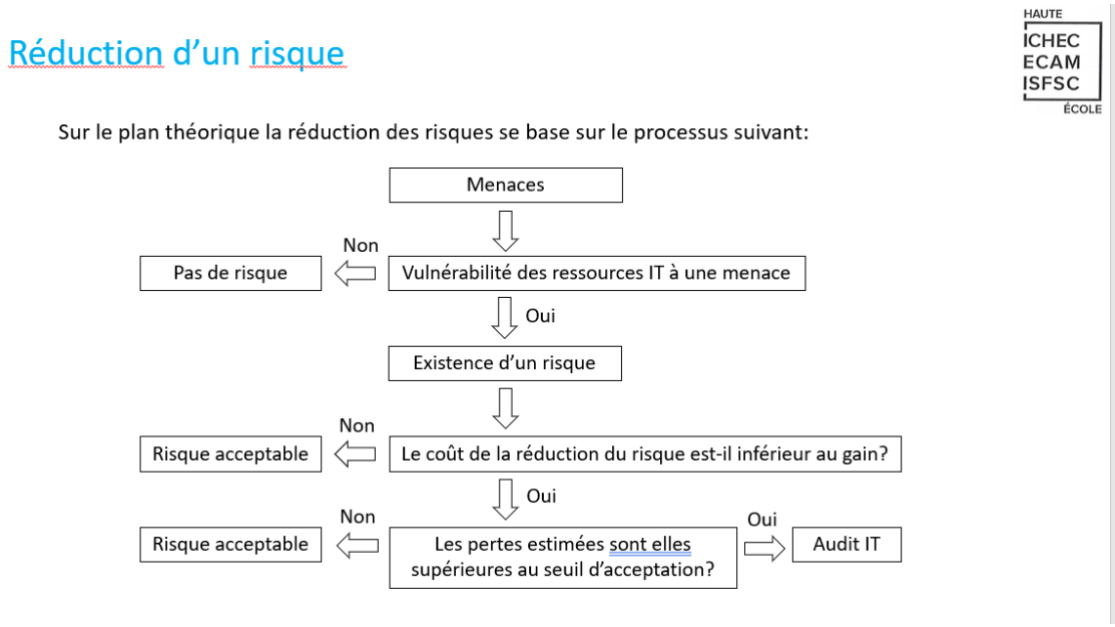


Figure 13: Réduction d'un risque
Source : Georgel. (2009). *Réduction d'un risque* [Présentation Power Point]. ICHEC.

2.5.3 COSO

Après avoir examiné les principes fondamentaux du processus de gestion des risques, il est essentiel de se pencher sur les cadres de référence spécifiques qui fournissent une structure détaillée pour une gestion efficace des risques. Parmi ces cadres, l'un des plus reconnus est le "Committee of Sponsoring Organizations of the Treadway Commission" (COSO).
COSO est une organisation à but non lucratif qui a élaboré des cadres de référence largement utilisés pour aider les entreprises à améliorer leur gestion des risques, leur contrôle interne et leur gouvernance d'entreprise. (Rédaction, 2019)

Selon le projet commandé par COSO, le cadre de référence, le "ERM - Integrated Framework", fournit une structure complète se concentrant sur la gestion des risques dans son ensemble, en fournissant des directives pour identifier, évaluer et gérer les risques à travers l'ensemble de l'entreprise. Il va être mis à jour quelques années après et va être renommé "ERM - Integrated with Strategy and Performance". Son but est d'élargir la perspective en mettant davantage l'accent sur l'alignement des risques avec la stratégie et les performances globales de l'organisation. Il cherche à intégrer la gestion des risques dans la prise de décision stratégique et à maximiser la création de valeur pour l'entreprise. En effet, la complexité des risques a évolué, de nouveaux risques sont apparus et les dirigeants et le conseil d'administration ont renforcé leur sensibilisation et leur surveillance tout en demandant une meilleure communication des risques.

L'objectif de la gestion des risques d'entreprise (ERM) est d'identifier, d'évaluer et de prioriser les risques pertinents pour l'organisation, qu'ils soient financiers, stratégiques ou opérationnels, afin de prendre des décisions éclairées sur leur gestion. Les plans de gestion des risques résultants doivent évaluer l'impact potentiel de ces menaces et détailler les réponses possibles en cas de réalisation d'un risque. Un processus ERM efficace revêt une importance stratégique pour les dirigeants d'entreprise. Les

informations sur les risques obtenues grâce à ce processus doivent être intégrées de manière significative dans le plan stratégique global de l'entreprise. (Kous, 2023)

Représentation du modèle COSO ERM 2017 :

Figure 14: ERM model

KOUS, H. (2023, 15 août). *COSO ERM 2017 traduit en français* [Diaporama]. Consulté le 14 février 2024, à l'adresse https://fr.slideshare.net/hassanekoussoubeKOUS/coso-erm-2017-traduit-en-franaispdf

Le modèle COSO ERM 2017 vise à fournir aux organisations un cadre actualisé et robuste pour la mise en œuvre de la gestion des risques à l'échelle de l'entreprise. Il met l'accent sur l'importance de la gestion des risques dans la création de valeur pour l'entreprise et dans la réalisation de ses objectifs stratégiques.

Les composantes du modèle sont les suivantes :

Gouvernance et culture est ce qui renforce l'importance et la compréhension de la gestion des risques dans l'entreprise, établit les responsabilités de supervision nécessaires pour la mener à bien et définit les valeurs éthiques.
Les principales actions à mener sont les suivantes :

- Approuver une politique à suivre par le Conseil d'administration pour superviser les risques de l'Entité.
- Établir la structure opérationnelle.
- Définir la culture et les valeurs souhaitées.
- La haute direction doit prouver son engagement envers les valeurs fondamentales en formant, par exemple, des comités et des organes collégiaux pour le contrôle de sa conformité.
- Attirer, développer et retenir un personnel qualifié.

Stratégie et fixation d'objectif est le processus de planification stratégique en définissant la gestion des risques de l'entreprise, les stratégies et les objectifs de travail.
Les principales actions à mener sont les suivantes :

- Analyser le contexte de l'activité.
- Définir l'appétit pour le risque.
- Évaluer les stratégies à suivre.
- Formuler des objectifs de l'entreprise.

Performance c'est l'identification et l'évaluation des risques qui peuvent affecter la réalisation des objectifs de l'entreprise. Les risques sont classés par ordre de priorité en fonction de leur gravité (voir figure 16 cartographies des risques), selon l'appétit pour le risque défini. L'organisation choisit ensuite des réponses aux risques et vérifie la quantité de risques qu'elle a pris.

Accomplir cette performance implique ce qui suit :

- Identifier les risques.
- Évaluer la gravité de chaque risque identifié.
- Identifier, sélectionner et mettre en œuvre des réponses aux risques.

Examen et suivi en examinant la performance l'entreprise vérifie le fonctionnement de la gestion des risques de l'entreprise au fil du temps et à la lumière des changements importants survenus, décide des révisions ou des modifications nécessaires.
Les principales actions à mener sont les suivantes :

- Évaluer les changements importants survenus.
- Examiner les risques et la performance au cours de leur gestion.
- Chercher à améliorer la gestion des risques.

Information, communication et rapports, la gestion des risques de l'entreprise exige un processus continu d'obtention et de partage des informations nécessaires provenant de sources internes et externes.
Les principales actions à mener sont les suivantes :

- Soutenir la gestion des risques à l'aide de systèmes et de technologies.
- Utiliser les canaux de communication appropriés.
- Informer toutes les parties prenantes sur les risques, la culture et la performance.

Chaque composante contient divers principes qui décrivent les actions et pratiques spécifiques requises. Toutefois, ces principes peuvent être appliqués de différentes manières par différentes organisations. Le COSO a également publié un supplément intitulé "Compendium of Examples", qui contient des études de cas sur la mise en œuvre du cadre ERM par des entités individuelles.

2.5.4 ISO 31000

Les normes ISO sont un ensemble de normes internationalement reconnues qui ont été créées dans le but d'aider les entreprises à établir des niveaux d'homogénéité en matière de gestion, de prestation de services et de développement de produits dans le secteur industriel. ISO est un groupe indépendant et non gouvernemental, qui a élaboré près de 25 000 normes internationales pour les systèmes de gestion. (ISO, 2022)

La norme ISO 31000 sur le management du risque propose des principes, un cadre et des directives pour gérer efficacement tous types de risques. Par exemple, panne d'équipement, accident d'un employé ou d'un client, atteinte à la cybersécurité et fraude financière. Elle est adaptée à toutes les organisations, quel que soit leur taille, leur secteur d'activité ou leur domaine d'expertise. En adoptant cette norme, les organisations peuvent évaluer leurs pratiques de gestion des risques par rapport à un référentiel international reconnu, garantissant ainsi un management et une gouvernance efficaces.

En plus de traiter les questions liées à la continuité opérationnelle, l'ISO 31000 aide les organisations à renforcer leur résilience économique, à protéger leur réputation professionnelle, à minimiser leur impact sur l'environnement, et à améliorer leur performance en matière de sécurité. (ISO, s. d.)

L'objectif principal est d'aider les organisations à protéger leurs actifs, à atteindre leurs objectifs et à améliorer la prise de décision. Elle se base sur 3 principales composantes qui sont : les principes, le cadre et le processus.

Les principes doivent être suivis par toute organisation qui souhaite mettre en œuvre un système de gestion de risque basé sur l'ISO 31000. Ils sont les suivants (voir figure 15 partie 4)

- **Intégration :** La gestion des risques doit être intégrée à tous les niveaux de l'organisation et à tous les processus.
- **Structurée :** La gestion des risques doit avoir une approche structurée dans la gouvernance de l'organisation.
- **Personnalisation :** La gestion des risques doit s'adapter aux besoins et aux caractéristiques spécifiques de chaque organisation.
- **Inclusion :** Toutes les parties prenantes pertinentes doivent participer au processus de gestion des risques.
- **Dynamisme :** La gestion des risques doit être proactive et capable de s'adapter aux changements dans l'environnement interne et externe.
- **Amélioration continue :** L'organisation doit constamment rechercher des opportunités pour améliorer son approche de gestion des risques.
- **Basée sur l'information :** La prise de décision en matière de gestion des risques doit être basée sur des informations précises et à jour.
- **Facteurs humains et culturels :** Le comportement humain et la culture influencent la gestion des risques.

Pour ce qui est du cadre de référence, il vise à aider les organisations à intégrer la gestion du risque dans l'ensemble de leur activité. (figure 15 partie 5)
Leadership et engagement de la haute direction : La direction joue un rôle crucial en alignant la gestion des risques avec les objectifs, la stratégie et la culture de l'organisation, et en assignant des responsabilités appropriées à tous les niveaux.

Intégration de la gestion des risques : Une compréhension approfondie de la structure et du contexte de l'organisation est essentielle pour intégrer efficacement la gestion des risques. La gouvernance et les structures de gestion traduisent la stratégie en actions concrètes pour une performance durable, tandis que chaque membre de l'organisation partage la responsabilité de gérer les risques.

Conception du cadre de référence : La conception du cadre de référence implique la compréhension du contexte interne et externe, l'engagement envers la gestion des risques, la définition des rôles et responsabilités, l'allocation de ressources et une communication efficace avec les parties prenantes.

Mise en œuvre du cadre de référence : Une mise en œuvre réussie nécessite un plan adéquat, l'identification des décideurs, la modification des processus pertinents, ainsi qu'une évaluation périodique des performances et une amélioration continue pour assurer l'efficacité du cadre de référence.

Adaptation continue du cadre de référence : L'organisation doit constamment ajuster et améliorer son cadre de référence en fonction des changements internes et externes, en identifiant les écarts et les opportunités d'amélioration, et en attribuant des responsabilités pour sa mise en œuvre.

La norme décrit le processus que les organisations doivent utiliser pour identifier, évaluer, hiérarchiser et atténuer les risques, avec des conseils sur la manière d'appliquer les politiques, les procédures et les pratiques de manière systématique. Elle prévoit également des étapes pour la communication, le suivi et l'examen, ainsi que l'établissement de rapports. (figure 15 partie 6)

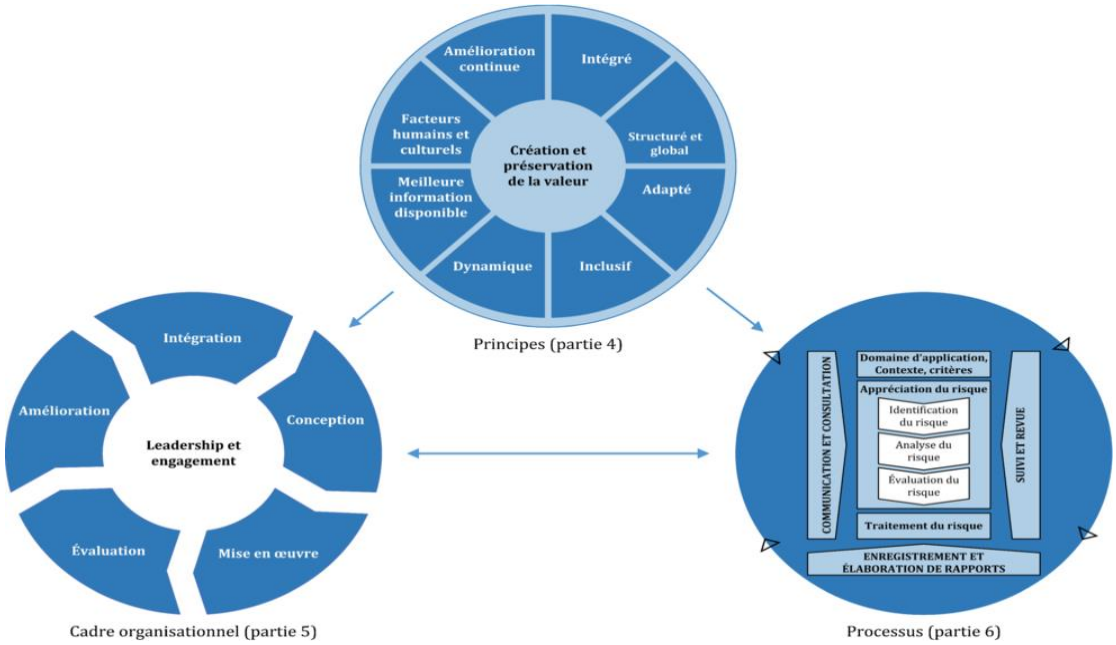


Figure 15: ISO 31000 principes, cadre et processus.

Source : GlobalSuite Solutions. (2023, 28 décembre). *Qu'est-ce que la norme ISO 31000 et à quoi sert-elle ? Découvrez l'importance de la gestion des risques au sein de votre organisation.* Consulté le 13 février 2024, à l'adresse https://www.globalsuitesolutions.com/fr/quest-ce-que-la-norme-iso-31000-et-a-quoi-sert-elle/

ISO 31000 et le cadre COSO partagent un objectif commun : aider les organisations à mettre en œuvre des stratégies efficaces de gestion des risques. Ils sont tous deux conçus pour s'adapter à toutes les organisations, indépendamment de leur secteur ou de leur industrie, et visent à formaliser les pratiques de gestion des risques dans toute l'entreprise. Cependant, leurs approches diffèrent. ISO 31000 se concentre principalement sur la gestion des risques et son rôle dans la planification stratégique et la prise de décision, tandis que le cadre COSO met davantage l'accent sur la gouvernance d'entreprise et l'audit des activités de gestion des risques. En outre, ISO 31000 est relativement concise, tandis que le cadre COSO est plus volumineux et détaillé, comprenant plus de 100 pages de texte et d'éléments visuels. En termes de public cible, ISO 31000 s'adresse à un large public intéressé par la gestion des risques, tandis que le cadre COSO est plus spécifiquement orienté vers les professionnels de la comptabilité et de l'audit. (Cobb, 2023)

En conclusion, il n'existe pas de méthode unique pour gérer un portefeuille de risques. Le cadre COSO ERM et la norme ISO 31000 peuvent tous deux aider les organisations à améliorer leurs pratiques ERM. L'un n'est pas nécessairement meilleur que l'autre, et des éléments des deux peuvent très bien être incorporés dans un système de gestion des risques.

2.5.5 ISO 27005

La norme ISO 27005 est particulièrement pertinente pour le chapitre sur la gestion des risques. En effet, cette norme fournit des lignes directrices pour la gestion des risques liés à la sécurité de l'information dans le cadre d'un Système de Management de la Sécurité de l'Information (SMSI). Contrairement à l'ISO 27001 qui se concentre sur la mise en place d'un SMSI, l'ISO 27005 se focalise spécifiquement sur les processus de gestion des risques.

La conformité à la norme ISO/IEC 27005 implique qu'une organisation a mis en place une approche systématique pour identifier, évaluer et traiter les risques liés à la sécurité de ses informations. Cette norme est essentielle dans le contexte de cette recherche, car elle permet de répondre aux défis posés par la cybercriminalité et les nouvelles menaces émergentes. En fournissant un cadre pour l'évaluation des risques, l'ISO 27005 aide les organisations à adopter une démarche proactive dans la gestion des risques (ISO, 2018).

L'application de l'ISO 27005 permet de protéger les informations sensibles de l'entreprise, telles que les données financières, personnelles et les propriétés intellectuelles. Elle renforce également la crédibilité de l'entreprise en rassurant les clients et les fournisseurs sur la robustesse de son système de gestion des risques. Cette norme oblige l'organisation à mettre en place des mécanismes de sécurité appropriés et à élaborer des plans de réponse aux incidents qui précisent les actions à entreprendre en cas de cyberattaque (ISO, 2018).

Face à l'augmentation de la cybercriminalité et à l'émergence constante de nouvelles menaces, l'ISO/IEC 27005 aide les organisations à comprendre les risques et à identifier et traiter de manière proactive les vulnérabilités. Elle offre les meilleures pratiques à adopter en termes de protection des données et de cyberrésilience, couvrant plusieurs aspects critiques de la gestion des risques. Cette norme permet aux organisations de tous les secteurs et de toutes tailles de gérer la sécurité de leurs actifs de manière efficace (ISO, 2018).
ISO 27005 est spécifique à la sécurité de l'information, tandis qu'ISO 31000 est généraliste et applicable à tous les types de risques.

Afin de se simplifier la tâche, il existe une cartographie des risques qui est un outil de management utilisé dans une démarche d'étude et de gestion du risque. Elle consiste à recenser les risques et à les synthétiser sur un document dans lequel ils seront placés en tenant compte de leurs impacts s'ils survenaient et de leurs fréquences hypothétiques.

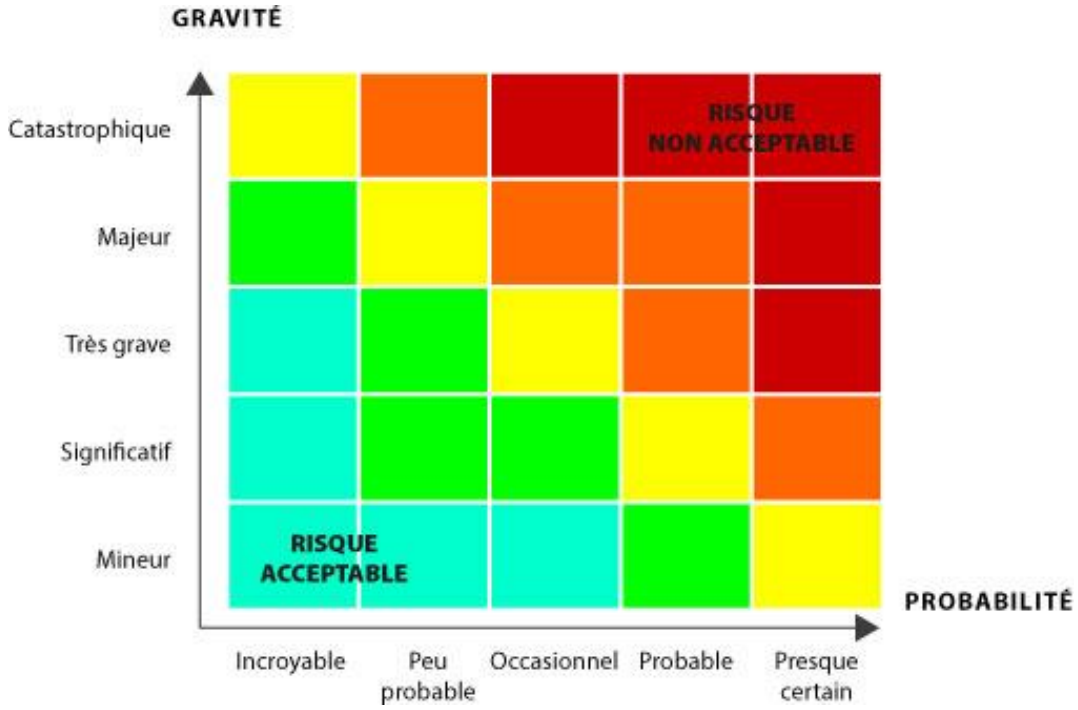


Figure 16: Cartographie des risques

Rizzon, Y. (2022, mars 22). *La cartographie des risques : pourquoi est-ce un outil indispensable ?* SDES. Consulté le 15 ovembre 2023, à l'adresse https://sdes.fr/fiches-pratiques/la-cartographie-des-risques-pourquoi-est-ce-un-outil-indispensable/

L'intérêt de ce tableau est de prendre connaissance de tout ce qui pourrait mettre en péril l'entreprise et également d'être réactif dans le cas où elles surviendraient. (Rizzon, 2022)

Il est de ce fait impératif d'établir un plan de gestion des risques dès les phases initiales de la mise en route du projet, car cela va permettre à l'entreprise de mettre en place sa stratégie plus facilement. L'entreprise pourra minimiser les pertes de temps et d'argent, et sera préparée à gérer efficacement le risque lorsqu'il surviendra.

2.5.6 NIST

Un autre cadre de gestion des risques cybernétiques très répandu aux États-Unis et dont beaucoup de frameworks s'inspirent est le NIST Cybersecurity Framework (CSF). Le NIST CSF a été publié pour la première fois en 2014 après une collaboration entre le gouvernement et le secteur privé, dans le but d'aider les organisations à mieux comprendre, gérer et réduire leur risque de cybersécurité et à protéger leur réseau et leurs informations. Le cadre est volontaire et conçu pour être applicable à des organisations de toutes tailles, dans tous les secteurs. Ce cadre, initié en 2013, a été développé en collaboration avec le secteur privé pour intégrer les meilleures pratiques de l'industrie. Il comprend plusieurs fonctions telles que l'identification, la protection, la détection, la réponse et la récupération, chacune comportant des catégories et des sous-catégories pour guider les actions de sécurité. Par exemple, la fonction d'identification aide à comprendre les actifs et les risques, tandis que la fonction de protection couvre les mesures de sécurité techniques et physiques. Le cadre offre également des références informatives pour corréler ses éléments avec d'autres normes et cadres de sécurité. Il est suffisamment flexible pour s'adapter aux besoins de toute organisation, permettant le choix des outils et des méthodes les plus appropriées pour renforcer la cybersécurité. (IBM, 2022)

Figure 17: NIST Framework
Source : National Institute of Standards and Technology. (s. d.). *NIST Cybersecurity Framework.* Consulté le 17 mars 2024, à l'adresse https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

2.5.7 Tableau de synthèse

Le tableau ci-dessous (tableau 3) sert de récapitulatif consolidé des quatres systèmes de référence majeurs : COSO, ISO 31000 et ISO 27001 et NIST. Chacun de ces cadres offre des structures distinctes pour une gestion optimale des risques, allant de la gouvernance d'entreprise aux spécificités de la sécurité de l'information. Par ce tableau, nous avons un aperçu comparatif qui souligne leurs objectifs, approches et domaines d'application respectifs, permettant aux organisations de choisir ou de combiner les éléments les plus pertinents pour leur gestion des risques. Ce tableau résume donc l'essentiel des connaissances acquises et constitue une référence pratique pour les décideurs souhaitant implémenter ou améliorer leur stratégie de gestion des risques.

Cadre de Gestion de Risque	Objectif	Approche	Application
COSO ERM (2017)	Aligner la gestion des risques avec la stratégie de l'organisation et améliorer la prise de décision	- Intégration dans la culture d'entreprise - Alignement avec la stratégie et la performance	Gestion d'entreprise, contrôle interne, assurance sur les objectifs d'entreprise
ISO 31000	Fournir des lignes directrices pour la gestion de tous types de risques	- Principe de management adapté - Cadre organisationnel - Processus de gestion	Toutes les organisations quelles que soient leur taille ou leur activité
ISO 27005	Fournir des lignes directrices pour la gestion des risques liés à la sécurité de l'information	- Approche systématique pour identifier, évaluer et traiter les risques - Processus de gestion des risques détaillé	Organisations qui gèrent des données sensibles, quel que soit leur taille ou leur secteur
NIST	Fournir un cadre pour améliorer la sécurité et la gestion des risques des systèmes d'information et de l'information	- Cadre basé sur le risque pour la sélection et l'implémentation de contrôles de sécurité - Processus d'autorisation et d'accréditation	Utilisé par les agences fédérales américaines et entités qui travaillent avec elles, mais applicable dans d'autres contextes

Tableau 3: Tableau récapitulatif des cadres de gestion de risque.

2.6 Gestion des incidents

2.6.1 Les enjeux

Dans l'environnement numérique et interconnecté actuel, la résolution des problèmes de cybersécurité nécessite une approche holistique ainsi que des solutions personnalisées pour garantir des résultats durables.
La multiplication des échanges de données et l'évolution des cybermenaces rendent la lutte de plus en plus difficile. Donc on ne peut plus se demander si un incident va se produire, mais plutôt quand va-t-il survenir.

Malgré tous les efforts consentis au niveau de la sécurité de l'information, une entreprise n'est jamais à l'abri d'une panne ou d'une attaque réussie qui peuvent nuire à l'intégrité, la confidentialité et la disponibilité de ses données, et cela même dans les entreprises les mieux protégées, comme vu précédemment avec Meta.

Dans tous les secteurs, les organisations dépendent largement de la technologie pour la réalisation de leurs activités. Les risques liés à la cybersécurité, inhérents à toute utilisation technologique, se manifestent de diverses manières et à travers de nombreuses sources. Les pannes informatiques, les applications obsolètes et leurs infrastructures de support sont parmi les situations les plus fréquentes, bien qu'évitables, pouvant conduire à des violations de données. Selon la dernière étude sur le coût des violations de données menée par l'Institut Ponemon, le coût moyen global d'un incident de sécurité s'élève à 3,92 millions de dollars, atteignant même 8,19 millions de dollars par violation pour les entreprises américaines. Entre les conséquences financières et les atteintes à la réputation, les répercussions d'un incident de cybersécurité peuvent être extrêmement difficiles à surmonter. (Ponemon Institute, & IBM Security, 2023).

Les entreprises ne sont donc pas forcément préparées à réagir à ce genre d'incident, le plus souvent elles apprennent à réagir aux incidents qu'une fois l'attaque subit. Ce manque de préparation pousse à avoir des réactions en temps réels dans des conditions qui ne sont pas optimales. Les entreprises ont donc tout intérêt à y être préparées. (Ejzyn, A., & Van den Berghe, T, 2019). Nombreuses sont les organisations qui ne possèdent pas l'expertise et les compétences nécessaires en interne pour réagir de façon appropriée en cas d'incident de cybersécurité. Lorsqu'elles sont confrontées à un incident, ces organisations peuvent avoir besoin de faire appel à des experts en vue de confiner l'incident, ce qui ne signifie pas qu'elles ne peuvent rien faire à leur niveau. Au contraire, beaucoup de choses peuvent et doivent entre faites en amont, avant qu'un incident ne survienne.

Il n'existe aucune solution simple et universelle, chaque organisation est différente. Ce qui fonctionne pour une organisation dépendra de sa mission et de ses objectifs, de la nature, de l'infrastructure et des informations qui sont protégés. Il faut savoir aussi que certaines techniques ne s'assimileront qu'avec le temps et l'expérience. Les incidents de cybersécurité représentent un risque qui doit être intégré à la politique globale de gestion des risques de l'organisation. En outre, il ne suffit pas d'apporter une réponse technologique. Il s'agit également de la mise en place d'un plan qui doit être intégré aux processus existants. L'humain est le maillon faible en matière de cybersécurité, mais il est aussi celui qui offre le potentiel réel à aider l'organisation à détecter et identifier les incidents. (CCB, 2016)

2.6.2 Processus de gestion des incidents

Il est essentiel de reconnaître l'importance de la préparation et de la réactivité face aux incidents de cybersécurité. À cet effet, le guide élaboré par le Centre for Cyber Security Belgium (CCB) souligne la nécessité d'adopter une approche proactive. Cette démarche est structurée autour d'un cycle méthodique comprenant différentes phases essentielles : la préparation, la détection, le confinement, l'atténuation, la reprise, et enfin, l'analyse post-incidents. Ce dernier volet est crucial, car il vise à capitaliser sur l'expérience acquise pour perfectionner le processus de gestion et renforcer la préparation face aux éventuels incidents futurs. La communication efficace avec toutes les parties prenantes, qu'elles soient internes ou externes, est également un aspect fondamental de ce cycle.

Dans ce contexte, l'adoption de cadres normatifs tels qu'ITIL (Information Technology Infrastructure Library) et COBIT (Control Objectives for Information and Related Technology) s'avère particulièrement pertinente. Ces référentiels offrent des lignes directrices et de meilleures pratiques pour la gestion des services informatiques, y compris la gestion des incidents. ITIL, avec son accent sur la gestion des services, propose un modèle qui facilite la gestion efficace des incidents en assurant une reprise rapide des services IT. De son côté, COBIT se concentre sur la gouvernance des TI, offrant un cadre qui permet d'aligner les processus IT avec les objectifs stratégiques de l'organisation, et inclut des pratiques de gestion des incidents pour assurer la résilience et la continuité des opérations.

2.6.2.1 ITIL

ITIL (Information Technology Infrastructure Library) est un ensemble de bonnes pratiques (best practices) largement documenté, portant sur la gestion et le support du système d'information. Il s'agit d'un référentiel qui offre des recommandations et un langage commun pour la fourniture de services informatiques aux clients internes et externes.
Elle se repose sur une approche par processus qui permet de disposer d'une base, de recommandations et d'un langage commun, offre un cadre reconnu, un référentiel qui apporte aux services informatiques, aux infrastructures, à la sécurité une organisation, une qualité, une efficacité, et qui réduit les risques.

Dans les années 80, le gouvernement britannique, en quête d'une série de standards pour optimiser les performances des services informatiques, a initié la création d'ITIL (Information Technology Infrastructure Library). Avec le temps, ITIL a gagné en popularité et a connu plusieurs évolutions, grâce à la publication de nouvelles versions adaptées aux changements du secteur. En 2019, ITIL 4 a été introduit, marquant un tournant dans la méthodologie avec une vision plus intégrée et flexible de la gestion des services informatiques (ITSM), adaptée aux besoins contemporains. (Grandmontagne, 2017)

ITIL v4 est la quatrième et dernière édition du guide informatique ITIL. Publiée en février 2019, elle succède officiellement à ITIL v3. Cette nouvelle version est principalement considérée comme une extension ou un perfectionnement de la précédente. Les principes fondamentaux d'ITIL v3 restent valables dans ITIL v4, avec un renforcement dans des domaines tels que la transparence, la collaboration et l'automatisation. (Ionos, 2021)

Modèle à quatre dimensions, ITIL v4 intègre ce modèle pour une approche plus holistique.
Les quatre dimensions sont :
Organisations et personnes : Comprends les rôles, les compétences et la culture.
Informations et technologies : Englobe les données, les systèmes et les outils.
Partenaires et fournisseurs : Inclus les relations externes.
Flux de valeur et processus : Se concentre sur la chaîne de valeur et les processus de gestion des services. (Figure 18)

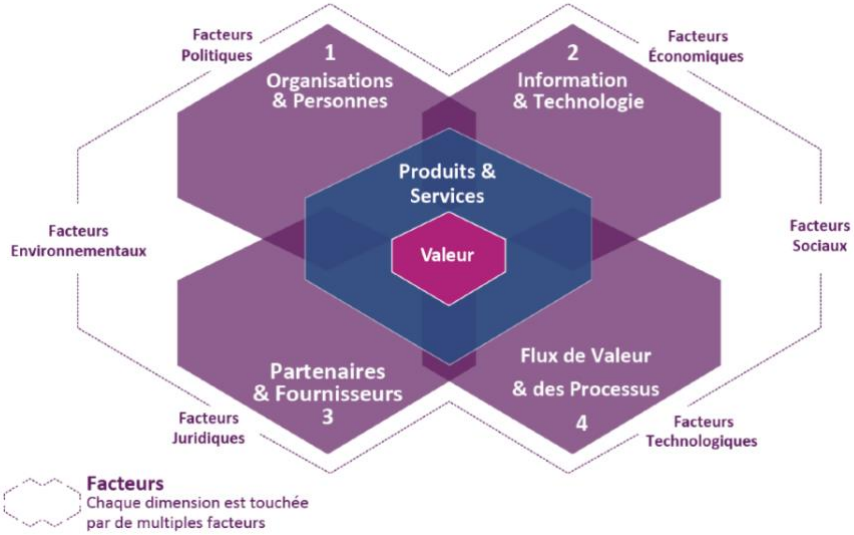


Figure 18: Modèle à 4 dimensions d'ITIL

QRP International. (2022, 28 juin). *ITIL c'est quoi ? Définition ITIL.* Consulté le 14 février 2024, à l'adresse https://www.qrpinternational.fr/blog/gestion-des-services-informatiques/itil-cest-quoi-definition-itil/

Dans le cadre ITIL, la gestion des incidents fait partie des étapes du cycle de vie de l'exploitation des services. La gestion des incidents désigne le processus utilisé par les équipes de développement et des opérations informatiques pour répondre à un événement imprévu ou une interruption de service et rétablir le fonctionnement du service.

Les incidents désignent tout événement qui, de manière effective ou potentielle, perturbe ou diminue la qualité d'un service. Ils peuvent se manifester sous diverses formes, qu'il s'agisse d'une défaillance d'une application critique pour l'entreprise ou d'un serveur web vieillissant opérant avec lenteur, compromettant ainsi la productivité. Dans le cas extrême, ce dernier pourrait même céder, provoquant une panne totale. L'éventail de la gravité des incidents est large, allant d'une interruption majeure affectant un service web à l'échelle globale jusqu'à des erreurs sporadiques touchant seulement une poignée d'utilisateurs.

La résolution d'un incident se produit quand le service impacté est rétabli à son fonctionnement normal. Cette résolution se concentre exclusivement sur les actions immédiates nécessaires pour minimiser l'impact sur les utilisateurs et restaurer les fonctionnalités du service. (Atlassian, s. d.)

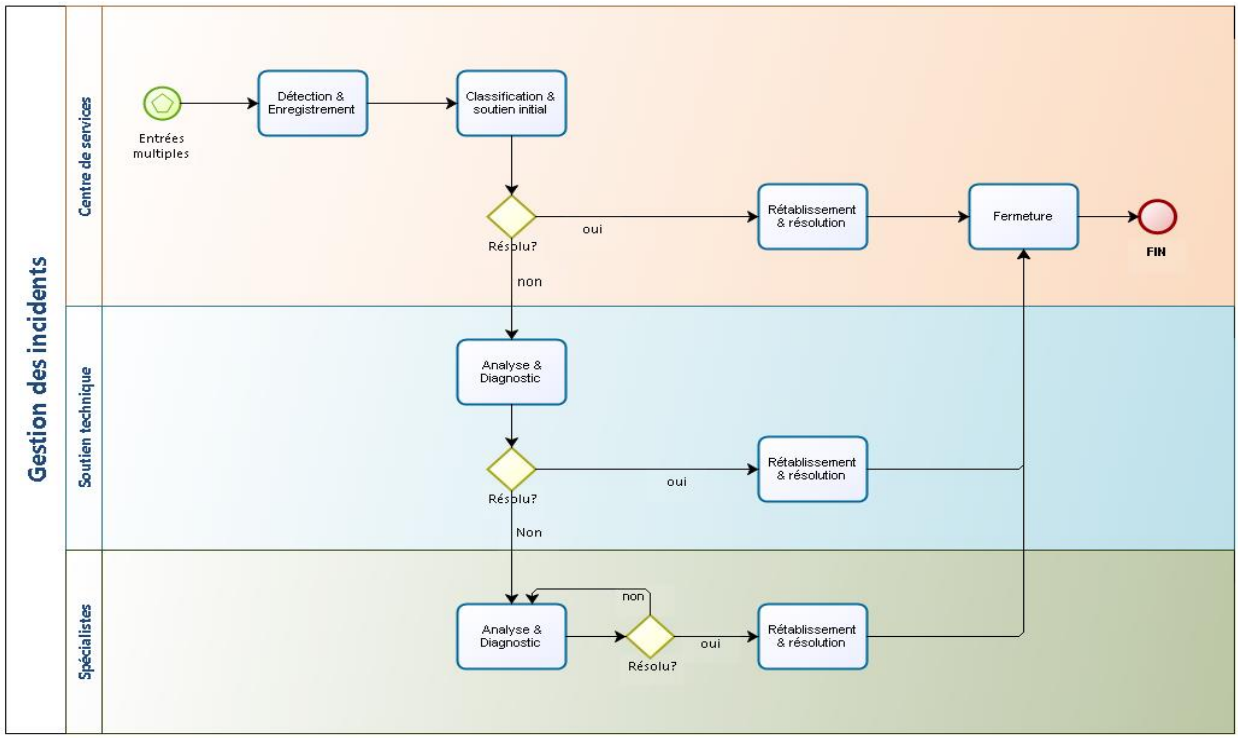


Figure 19: Exemple de processus ITIL pour la gestion d'incident
Octopus. (s. d.). *Gestion des incidents - Processus ITIL*. Consulté le 13 avril 2024, à l'adresse https://docs.octopus-itsm.com/fr/articles/gestion-des-incidents-processus-itilr

Elle constitue donc un élément clé de la gestion des services informatiques (ITSM). Ce processus est conçu pour assurer que les organisations puissent rétablir leurs opérations normales dans les plus brefs délais, en minimisant, autant que possible, les répercussions négatives sur leurs activités principales. Dans ce contexte, il est souvent nécessaire d'adopter des solutions temporaires pour pallier immédiatement les problèmes, tandis que l'identification de la cause profonde des incidents peut s'effectuer ultérieurement. Les incidents sont journalisés et le processus de résolution est enregistré. (TOPdesk, 2023)

Obtenir la certification ITIL est une initiative précieuse pour les professionnels de l'informatique et les organisations qui souhaitent améliorer leurs capacités de gestion des services informatiques. La certification ITIL permet aux individus de bien comprendre les pratiques et les principes d'ITIL et d'acquérir les connaissances et les compétences nécessaires pour contribuer à l'efficacité des opérations informatiques et à la prestation de services.

2.6.2.2 COBIT

COBIT (Control Objectives for Information and Related Technologies) est un cadre de gouvernance IT élaboré par l'ISACA pour aider les entreprises à gérer et à gouverner leurs technologies de l'information de manière holistique.

La gestion des risques dans COBIT permet aux organisations de faire face aux incertitudes liées à la TI, en identifiant, évaluant et gérant efficacement les risques informatiques susceptibles d'affecter l'entreprise. COBIT encourage l'identification proactive des risques grâce à une approche structurée et intégrée, assurant que les décisions de gestion tiennent compte de la tolérance au risque et des appétits de risque de l'organisation. (Suganya, 2019)

COBIT 5, introduit en 2012, visait à intégrer les aspects de la gouvernance des TI avec les préoccupations commerciales générales, mettant l'accent sur la création de valeur pour l'entreprise grâce à une utilisation efficace et innovante des technologies de l'information. Depuis COBIT 5 jusqu'à la version de 2019, ce cadre a connu plusieurs évolutions majeures. COBIT 2019 présente une intégration plus étroite avec d'autres cadres de travail et normes de l'industrie, telle qu'ITIL et ISO/IEC 27001, pour une approche plus cohérente de la gouvernance des TI. Il met également davantage l'accent sur la gouvernance des TI dans un contexte de transformation digitale rapide et de perturbation technologique. (Hurkadli, 2023).

Les 6 principes d'un système de gouvernance dans l'univers de COBIT 2019, constituent le Framework orientant les utilisateurs de COBIT dans la bonne direction. Les principes expriment non seulement de bonnes intentions, mais aussi que tout ce que les praticiens font doit être aligné sur ces principes.

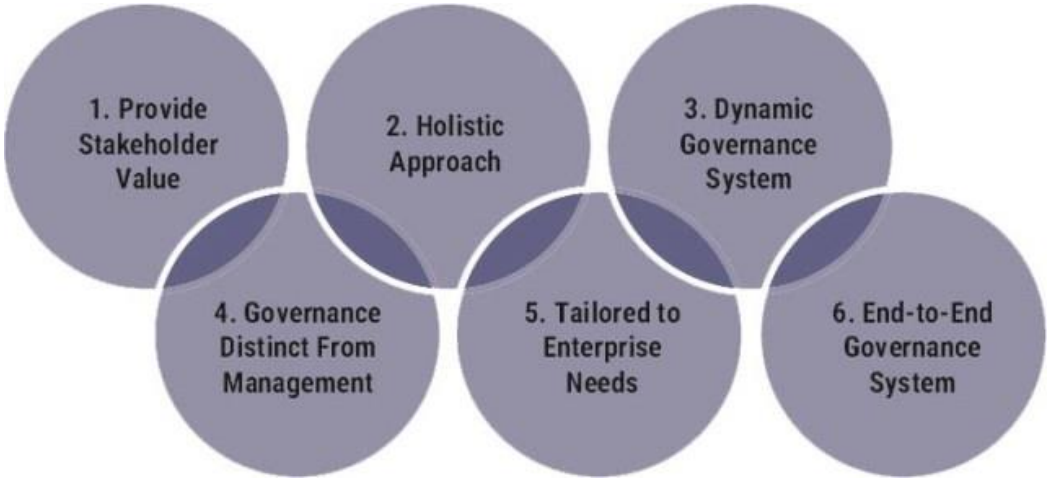


Figure 20: COBIT 2019 Framework: Introduction and Methodology
Bonneaud, A. (2019, 4 mars). *Guide COBIT 2019 : de A jusqu'à Z*. Blog de la Transformation Digitale. Consulté le 2 avril 2024, à l'adresse https://www.ab-consulting.fr/blog/cobit-2019/guide-cobit-2019-de-a-jusqua-z

Le modèle central de COBIT 2019 regroupe l'ensemble des 40 objectifs de gouvernance et de management de l'information et de la technologie.

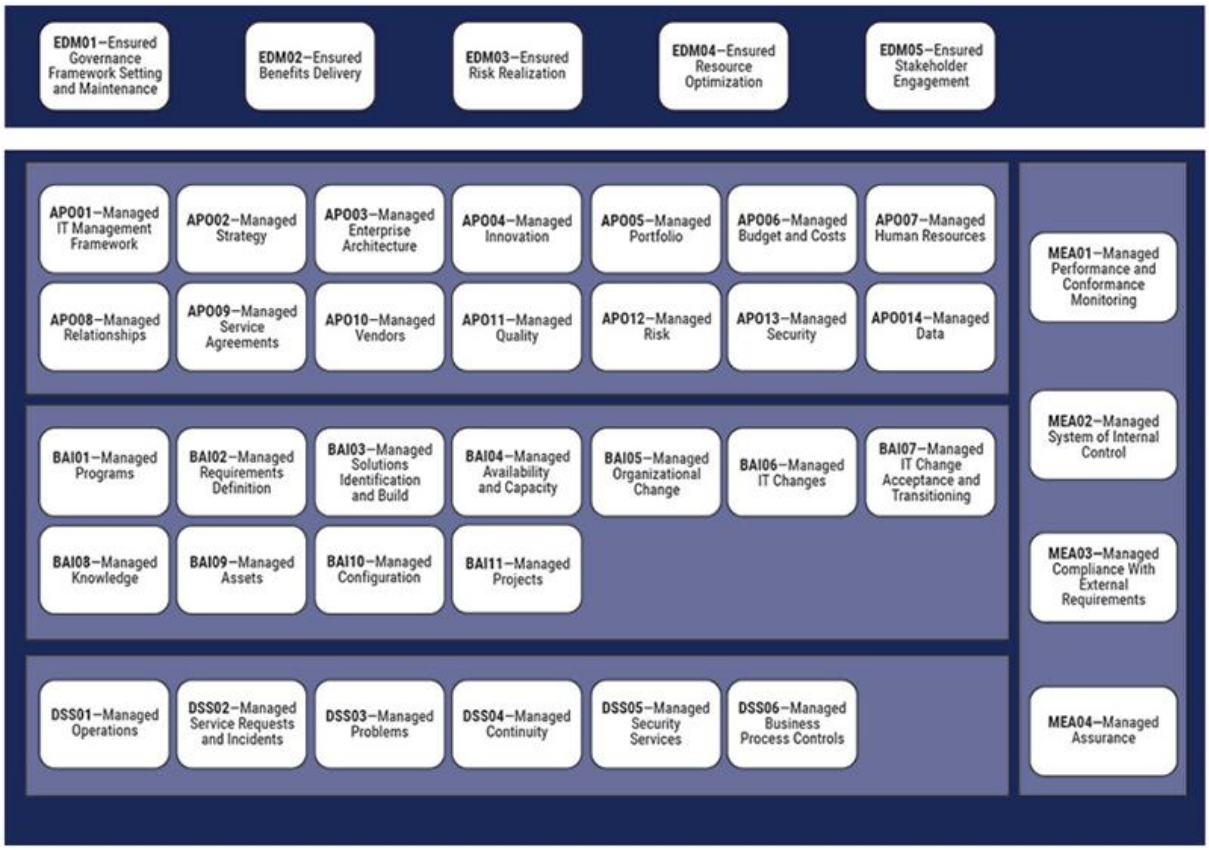


Figure 21: COBIT Core Model, COBIT 2019 Framework,
Bonneaud, A. (2019, 4 mars). *Guide COBIT 2019 : de A jusqu'à Z.* Blog de la Transformation Digitale. Consulté le 2 avril 2024, à l'adresse https://www.ab-consulting.fr/blog/cobit-2019/guide-cobit-2019-de-a-jusqua-z

COBIT propose des objectifs de contrôle et des bonnes pratiques pour aider les organisations à établir et à maintenir un environnement informatique sûr et fiable. Ainsi, Cobit peut être utilisé comme un outil pour mettre en œuvre les exigences de sécurité de la directive NIS 2. En utilisant COBIT, les organisations peuvent identifier et mettre en œuvre les contrôles de sécurité nécessaires pour se conformer aux exigences de la directive NIS 2, tout en bénéficiant d'une approche structurée et basée sur les bonnes pratiques pour la gouvernance et la gestion des TI.

En ce qui concerne la gestion des incidents dans le cadre COBIT, celle-ci est traitée comme une partie intégrante du processus de gouvernance et de gestion de l'information et des technologies de l'organisation. COBIT recommande la mise en place de pratiques et de procédures spécifiques pour répondre efficacement aux incidents informatiques. Ces procédures sont conçues pour détecter rapidement les incidents, les résoudre de manière efficiente et minimiser leur impact sur les opérations de l'entreprise.

La gestion des incidents selon COBIT inclut l'établissement de mécanismes de détection et de communication des incidents, ainsi que la définition des rôles et responsabilités pour une réponse coordonnée. Cela comprend également l'analyse post-incident pour en tirer des enseignements et améliorer continuellement les processus de gestion des incidents.

La structure de COBIT intègre des objectifs de contrôle et des indicateurs de performance clés (KPI) pour mesurer l'efficacité des processus de gestion des incidents, garantissant que les organisations disposent d'une vue d'ensemble sur la manière dont les incidents sont gérés et sur la capacité de l'entreprise à maintenir la continuité des opérations. (Bonneaud, 2019)

2.6.3 Tableau de synthèse

ITIL et COBIT se positionnent comme des références incontournables, offrant des pratiques éprouvées et une structure pour une réponse organisée et efficace. Le tableau suivant met en lumière la comparaison entre ces deux cadres en ce qui concerne leur approche de la gestion des incidents. Chaque colonne décrit les particularités, les principes et les processus prescrits par ITIL et COBIT, illustrant ainsi leur contribution à la résilience organisationnelle face aux cybermenaces.

Aspects	ITIL	COBIT 2019
Objectif	Gestion efficace des incidents pour rétablir rapidement les services IT	Alignement des processus IT avec les objectifs stratégiques pour la résilience des opérations
Approche	Gestion des services à travers un cycle de vie	Gouvernance IT holistique avec gestion des risques
Modèle	ITIL 4 adopte un modèle à quatre dimensions pour une approche holistique	COBIT 2019 intègre un modèle central pour gouvernance et gestion de l'IT
Gestion des incidents	Processus clé dans le cycle de vie de l'exploitation des services	Partie intégrante de la gouvernance et de la gestion de l'information et des technologies
Implémentation	Processus standardisé avec un langage commun	Objectifs de contrôle avec intégration de bonnes pratiques pour la sécurité IT
Évolution	D'ITIL v3 à ITIL v4, avec renforcement de la transparence, collaboration, et automatisation	De COBIT 5 à COBIT 2019, intégration avec d'autres cadres et normes industrielles
Analyse post-incident	Étape cruciale pour perfectionner le processus de gestion et renforcer la préparation	Analyse pour tirer des enseignements et améliorer les processus de gestion des incidents
Réactivité	Modèle qui facilite une reprise rapide des services	Recommande des procédures spécifiques pour une réponse efficace aux incidents
Ciblage des problèmes	Divers incidents de service, du critique au mineur	Incertitudes TI et gestion des risques informatiques affectant l'entreprise

Tableau 4: Tableau récapitulatif des cadres de gestion des incidents.

2.7 Directive NIS

L'examen minutieux des réglementations clés de l'Union européenne constitue une plateforme solide pour la transition vers une analyse approfondie de la directive NIS 2. Comprendre le RGPD, DORA, CSA et CRA a permis de contextualiser l'importance croissante de la cybersécurité et de la résilience numérique au sein de l'UE. Cette exploration a établi une fondation conceptuelle et réglementaire qui mène naturellement à la directive sur la sécurité des réseaux et des systèmes d'information, connue sous le nom de NIS 2.

La directive NIS 2, qui élargit et renforce la première directive NIS, vise à établir un niveau élevé commun de sécurité des réseaux et des systèmes d'information à travers l'Union. En plaçant le NIS 2 dans le contexte de ces directives existantes, il est possible de saisir l'évolution des priorités réglementaires et des attentes en matière de sécurité. Cela offre non seulement un aperçu des interactions entre différentes initiatives législatives, mais aussi une première compréhension de la manière dont le NIS 2 s'intègre et se distingue au sein de ce cadre.

Avec cette base préliminaire, je peux désormais aborder le NIS 2 non seulement avec un sens de sa portée et de son objectif, mais aussi avec une appréciation de son rôle dans l'harmonisation et l'amélioration des efforts de cybersécurité en Europe. La directive est ainsi présentée dans un contexte qui souligne sa pertinence et son urgence dans le paysage actuel de la sécurité numérique.

Les informations présentées dans ce chapitre s'appuient sur des documents trouvés en ligne ainsi que sur des entretiens réalisés avec des experts. Ces experts m'ont apporté des éclaircissements sur certains aspects complexes de la directive.

2.7.1 Contexte et émergence de la directive NIS

Au début des années 2010, le paysage numérique en Europe et dans le monde a connu une croissance exponentielle, avec une dépendance accrue aux technologies de l'information et de la communication (TIC) et face également à la multiplication des attaques visant les systèmes d'information, les cybercriminels et les acteurs étatiques malveillants ciblent désormais de manière privilégiée les vols de données et les violations de la vie privée. Les infrastructures critiques, telles que les réseaux électriques, les systèmes de transport, et les services de santé, sont devenues des objectifs privilégiés de ces attaques. C'est dans ce contexte que l'Union européenne a pris conscience de l'importance et l'urgence d'améliorer la sécurité des réseaux et des systèmes d'information pour aider ses citoyens et ses entreprises contre les risques croissants de cyberattaques. La stratégie de cybersécurité de l'Union européenne, dévoilée en 2013, a souligné le besoin impérieux d'un cadre juridique robuste pour renforcer la cybersécurité à travers l'Union et pour encourager la collaboration entre les États membres.

Pour répondre à ces enjeux, la directive NIS a été conçue et adoptée. Elle visait à unifier les différentes politiques nationales en matière de cybersécurité. Avant son instauration, l'absence d'harmonisation entre les pays membres de l'UE entravait considérablement la coopération internationale et la gestion des incidents cybernétiques à un niveau européen. (Provigis, s. d.)

Ces objectifs s'inscrivent dans la lignée des valeurs de l'Europe qui vise à offrir aux citoyens de l'Union européenne un espace ouvert, unifié où les législations internes de chaque État membre sont

harmonisées, mais également un espace physique et numérique sécurisé, où la sécurisation des réseaux informatiques en Europe se fait au bénéfice des citoyens européens autant que des entreprises (Quéméner, 2016).

2.7.2 Présentation de la directive NIS 1

Entrée en vigueur en août 2016, elle a été le premier véritable effort législatif à l'échelle de l'Union européenne pour renforcer la cybersécurité au sein des États membres. Avec pour objectif d'assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information, elle précise également les obligations qui incombent aux opérateurs en matière de sécurité informatique. Elle a été transposée dans la législation nationale, en Belgique, via la loi NIS du 7 avril 2019. (Provigis, s. d.)

Selon les premiers points de la directive publié par le parlement européen, il considérait que les réseaux et les services et systèmes d'information jouent un rôle crucial dans la société. Leur fiabilité et leur sécurité sont essentielles aux fonctions économiques et sociétales et notamment au fonctionnement du marché intérieur.

L'étendue, la fréquence, et les conséquences des incidents de sécurité ne cessent d'augmenter, posant une menace significative pour le bon fonctionnement des réseaux et des systèmes d'information. Ces systèmes peuvent également être la cible d'actions malveillantes intentionnelles visant à les compromettre ou à les interrompre. Ces incidents peuvent entraver les activités économiques, entraîner d'importantes pertes financières, ébranler la confiance des utilisateurs, et causer des préjudices considérables à l'économie de l'Union européenne. (Parlement européen, 2016).

Le champ d'application de la directive NIS 1 couvrait deux catégories d'acteurs :
Les opérateurs de services essentiels (OSE), des entreprises et organisations qui jouent un rôle crucial dans le fonctionnement de l'économie et de la société, notamment au travers de leur Système d'Information essentiel (SIE). Pour être classée comme OES au titre de la directive NIS, une entité doit répondre à trois critères. Elle doit fournir un service essentiel au maintien d'activités sociétales et économiques critiques. La fourniture du service doit reposer sur des réseaux et des systèmes d'information. Un incident de sécurité perturberait considérablement le service fourni. Comme les acteurs des secteurs de l'énergie, des transports, de la santé, de l'eau et des services financiers.

Les fournisseurs de services numériques (FSN), parfois désignés par l'acronyme DSP, pour Digital Service Provider. Il s'agit d'une organisation qui offre certains services numériques, comme des moteurs de recherche, des plateformes de vente en ligne et des fournisseurs de services de Cloud Computing. Toutefois, les FSN ne sont pas soumis aux mêmes exigences strictes de conformité que les OSE, à moins qu'ils ne dépassent un certain seuil en termes d'effectifs et de chiffre d'affaires. (Wavestone, 2018)

Figure 22: Devoir des états membres

Source : Wavestone. (2018, septembre). *De NIS 1 à NIS 2 : l'évolution (majeure) du cadre législatif européen en matière de cybersécurité*. Consulté le 14 février 2024, à l'adresse https://www.riskinsight-wavestone.com/2018/09/bilan-directive-nis/

La NIS 1 astreint les États membres à élaborer des stratégies nationales de cybersécurité et à collaborer de manière transfrontalière, via le NIS-Cooperation Group et le réseau CSIRT. La directive oblige en outre les États membres à identifier les opérateurs de services essentiels (OSE) dans au moins sept secteurs clés : l'énergie, les transports, les banques, les infrastructures des marchés financiers, la santé, l'eau potable et les infrastructures numériques. Ces opérateurs doivent prendre des mesures de sécurité minimales et signaler les incidents majeurs. Les fournisseurs (à partir d'une certaine taille) de services numériques essentiels, tels que les services dans le cloud, les moteurs de recherche et les marchés en ligne, doivent également se conformer à ces exigences de sécurité et de notification. (Byttebier, 2022)

2.7.3 Les limites de la directive NIS 1

La directive NIS 1 présente plusieurs limites. Tous les secteurs critiques n'étaient pas inclus dans son champ d'application, notamment la santé, les transports, l'énergie et les communications électroniques. Ainsi, les obligations de sécurité des réseaux et des systèmes d'information n'étaient pas uniformes dans tous les secteurs essentiels (Bourgin, 2024).

Le coût moyen d'une violation dans le secteur de la santé a atteint près de 11 millions de dollars en 2023, soit une augmentation de 53 % par rapport à 2020 (IBM, 2023). Les cybercriminels utilisent les données volées pour exercer une pression accrue sur les victimes, rendant les données médicales particulièrement vulnérables.

Un exemple notable est l'attaque contre UnitedHealth, revendiquée par le groupe BlackCat, qui a perturbé le traitement des réclamations d'assurance et les demandes pharmaceutiques aux États-Unis et en Europe, touchant 15 milliards de transactions de soins par an (Bourgin, 2024).

De plus, la directive NIS 1 permettait à chaque État membre de définir individuellement les Opérateurs de Services Essentiels (OSE), conduisant à des incohérences et des lacunes importantes. Cette fragmentation des normes de sécurité à travers l'Union européenne a compromis l'efficacité des mesures de sécurité et la coordination des réponses aux incidents transfrontaliers.

La supervision de la mise en œuvre de la directive était souvent inefficace, et la coopération entre les États membres restait limitée et ad hoc, entravant la protection des infrastructures critiques et l'échange d'informations sur les menaces et les incidents de sécurité (Bourgin, 2024).

2.7.4 Évolution vers la directive NIS 2

Pour appréhender avec exactitude la portée de la directive NIS 2, une étude de ses considérants s'avère indispensable. Ces énoncés fournissent une vision détaillée des objectifs, des préoccupations et des attentes législatives, permettant ainsi de contextualiser la genèse de la directive et de comprendre les enjeux de cybersécurité qu'elle vise à adresser. En examinant ces considérants, les organisations peuvent interpréter efficacement les exigences de la directive et élaborer des stratégies de mise en conformité adaptées, assurant ainsi une gouvernance conforme et une continuité opérationnelle optimale au sein de l'UE. Ces considérants n'ont aucune valeur juridique, mais ils permettent de donner une idée de pourquoi cette loi a été décidée, quel est l'esprit derrière.

Les considérants :

Selon la directive publié sur le site du Parlement européen et Conseil de l'Union européenne (2022), d'abord, elle vise à renforcer la résilience cybernétique de l'UE en couvrant davantage de secteurs essentiels et en encourageant une coopération accrue entre les États membres. Elle étend sa portée à plus d'entités économiques, unifiant les critères d'identification des opérateurs de services essentiels et fournisseurs de services numériques pour une meilleure clarté juridique. En révisant les déficiences de la directive précédente, elle aspire à une application plus cohérente et à une amélioration significative de la cybersécurité à travers l'UE.

Les considérants soulignent que l'évolution rapide des technologies numériques a augmenté la surface d'attaque et que les menaces sont devenues plus complexes et plus fréquentes, ce qui nécessite une réponse réglementaire plus robuste. Durant l'introduction de ce mémoire, j'ai eu l'occasion de présenter différents cas et exemple de cette expansion des attaques et l'enjeu autour de l'importance de la cyberrésilience.

La Commission européenne, dans l'évaluation de la directive NIS, a donc constaté des progrès significatifs en matière de cybersécurité. Cependant, le réexamen a mis en évidence des lacunes par rapport aux menaces contemporaines. L'augmentation des cybermenaces, soulignée dans la stratégie de cybersécurité de l'UE, appelle à un renforcement de la résilience et à l'assurance que les technologies numériques sont fiables pour les citoyens et les entreprises. La commission a également relevé un manque de clarté concernant la portée et les compétences, une mise en œuvre inefficace, des divergences considérables entre les approches nationales et un partage d'informations insuffisant.

La directive NIS 2 propose des changements significatifs visant à remédier aux lacunes identifiées et à renforcer la cybersécurité à l'échelle de l'Union européenne. Ces changements clés reflètent une volonté de garantir une protection plus cohérente et efficace des infrastructures critiques.

Le Parlement et le Conseil européens, malgré des divergences sur certains points, ont adopté la directive NIS 2 et elle est entrée en vigueur le 16 janvier 2023 et doit être transposée dans la loi belge pour le 17 octobre 2024.

Cette nouvelle directive ambitionne d'élargir la portée d'application à de nombreux acteurs de secteurs variés tels que la santé, l'infrastructure numérique, les transports et l'énergie, et de renforcer la gestion des risques et des incidents.

Les objectifs :

En essence, la directive NIS2 vise les mêmes objectifs que la directive initiale : **contraindre les autorités nationales à se concentrer sur un niveau plus élevé de la cybersécurité et de la résilience au sein des organisations de l'Union européenne, améliorer la coopération européenne en matière de cybersécurité, et exiger des opérateurs clés dans des secteurs essentiels qu'ils adoptent des mesures de sécurité et signalent les incidents.**
Les nouveautés principales résident dans **l'extension significative du champ d'application, une définition plus précise des mesures à prendre, des règles de notification d'incidents plus détaillées, des sanctions plus strictes et spécifiques, et une augmentation de la responsabilité des cadres dirigeants**, faisant de la cybersécurité un sujet de gouvernance central. (Lexing, 2023)

On retrouve, l'inclusion automatique dans le champ d'application du règlement, sans nécessité d'enregistrement préalable. Cela signifie que les entités considérées comme critiques seront automatiquement soumises aux exigences de cybersécurité établies par le règlement, sans avoir besoin de s'inscrire ou de se déclarer auprès des autorités compétentes.

L'extension du champ d'application du NIS 2 avec l'introduction d'un critère de taille implique que la directive vise à inclure un plus large éventail d'entités dans son périmètre réglementaire. Contrairement au NIS 1, où l'identification des Opérateurs de Services Essentiels (OSE) était laissée à la discrétion des États membres sans ligne directrice claire, le NIS 2 propose l'introduction d'un critère de taille pour déterminer quelles entités doivent être considérées comme critiques en termes de sécurité des réseaux et des systèmes d'information.

La directive liste en sa première annexe les secteurs considérés comme « hautement critiques », comme l'énergie, les transports ; le secteur bancaire et les infrastructures de marchés financiers, la Santé, l'eau potable et les eaux usées, les infrastructures numériques, etc. La deuxième annexe liste quant à elle les « autres secteurs critiques » comme les services postaux et d'expédition, la gestion des déchets, la fabrication, production et distribution de produits chimiques. La différence entre les termes "secteur critique" et "hautement critique" dans le contexte de la directive NIS 2 réside dans le niveau d'importance et l'impact potentiel sur la société et l'économie en cas de perturbation ou d'attaque contre des entités appartenant à ces secteurs.
Ensuite elle définit également les entités « essentielles » et « importantes ». (figure 23)

Figure 23: Scope des entités essentielles et importantes

Source : Scheelen, Y., Machilsen, K., & Deprez, A. (2023, 16 mai). *How to prepare for the NIS2 Directive ?* EY. Consulté le 6 mars 2024, à l'adresse https://www.ey.com/en_be/cybersecurity/how-to-prepare-for-the-nis2-directive

Une entité type figurant dans les annexes relève du champ d'application de la directive si elle est une grande ou moyenne entreprise, c'est-à-dire qu'elle occupe au moins 50 personnes ou réalise un chiffre d'affaires annuel d'au moins 10 millions d'euros.
La différence entre les entités essentielles et les entités importantes réside principalement dans la rigueur du contrôle et des sanctions. Les entités essentielles seront contrôlées et sanctionnées de manière plus stricte que les entités importantes. (Figure 24)

Il existe toutefois quelques exceptions. Dans certains secteurs, les entités sont catégorisées, quelle que soit leur taille, comme « essentielles » : par exemple, les fournisseurs de réseaux de communications électroniques publics, les entités identifiées comme critiques au niveau national en vertu de la directive CER, les entités de l'administration publique (au niveau central), les prestataires de services de confiance qualifiés et les registres de noms de domaines de premier niveau ainsi que les fournisseurs de services DNS. (CCB, 2024-c).

	Secteurs hautement critiques	Secteurs critiques
Grandes entreprises	Entités essentielles	Entités importantes
Moyennes entreprises	Entités importantes	Entités importantes
Petites entreprises Micro-entreprises	X	X

Figure 24: Entités essentielles ou importantes

Source : Lexing. (2023, 16 novembre). *Directive NIS 2 : quels changements anticiper ?* Consulté le 19 février 2024, à l'adresse https://lexing.be/directive-nis-2-quels-changements-anticiper/

La directive NIS 2 introduit plusieurs mesures spécifiques pour renforcer la cybersécurité des infrastructures critiques. Ces mesures incluent des directives, des protocoles et des recommandations concernant la protection contre les cyberattaques, la détection des incidents, la gestion des vulnérabilités et la sécurisation des données. L'objectif est de renforcer la résilience et la protection des infrastructures critiques contre les cybermenaces.

Responsabilité du management : Les dirigeants et hauts responsables d'une organisation doivent prendre en charge la sécurité des réseaux et des systèmes d'information. Cela inclut la définition des politiques de sécurité, l'allocation des ressources, la supervision des mesures de sécurité et la gestion des risques liés à la cybersécurité. L'engagement des dirigeants est crucial pour la protection des infrastructures critiques contre les cybermenaces (Lexing, 2023).

Notification des incidents : Contrairement à la directive NIS 1, la directive NIS 2 harmonise et renforce les obligations de notification des incidents de cybersécurité à l'échelle de l'Union européenne. Les entités devront signaler un éventail plus large d'incidents, y compris ceux ayant un impact sur des secteurs cruciaux pour l'économie et la sécurité nationale. Cela vise à améliorer la réactivité des autorités et la coordination des réponses aux incidents de cybersécurité transfrontaliers.

Renforcement et collaboration des CSIRT nationaux : La directive NIS 2 prévoit l'autonomisation et la collaboration accrue des équipes nationales de réponse aux incidents de sécurité informatique (CSIRT). Cela inclut des investissements dans la formation du personnel, l'amélioration des outils de surveillance et de réponse aux menaces, ainsi que le renforcement des partenariats entre entités gouvernementales et privées impliquées dans la cybersécurité.

La directive NIS 2 remédie aux lacunes de la directive NIS 1 et renforce la cybersécurité à l'échelle de l'Union européenne. Les changements clés incluent l'extension automatique du champ d'application, l'introduction de critères de taille pour déterminer les entités critiques, des mesures spécifiques de cybersécurité, la responsabilité accrue des dirigeants, et des obligations de notification étendues. Ces mesures visent à améliorer la détection, la réponse et la coordination des efforts de cybersécurité à travers les États membres, renforçant ainsi la résilience de l'UE face aux cybermenaces.

2.7.5 Tableau comparatif

Ce tableau synthétise les différences entre la première directive NIS et la directive révisée NIS 2, soulignant les améliorations et les changements visant à renforcer la sécurité des réseaux et des systèmes d'information au sein de l'Union européenne.

Aspect	Directive NIS 1	Directive NIS 2
Champ d'application	Défini par chaque État membre, sans ligne directrice claire. Ne couvre pas tous les secteurs jugés essentiels. 6 secteurs	Champ d'application élargis avec inclusion automatique des entités critiques selon des critères de taille et d'impact. 17 secteurs
Identification des entités	Les OSE sont identifiés par chaque État membre de manière ad hoc.	L'identification des entités importantes est plus structurée avec des critères précis.
Mesures de sécurité	Obligations en matière de sécurité non uniformes, pouvant varier d'un État à l'autre.	Introduction de mesures de cybersécurité spécifiques et harmonisées à l'échelle de l'UE.
Responsabilité du management	Peu de directives claires sur la responsabilité du management en matière de sécurité des réseaux et systèmes.	Reconnaissance explicite de la responsabilité de la direction dans la mise en œuvre de la cybersécurité.
Notification des incidents	Règles de notification des incidents variables et souvent limitées à des impacts significatifs.	Obligations étendues et harmonisées pour la notification d'un éventail plus large d'incidents de cybersécurité.
Supervision et conformité	Supervision incohérente et application limitée des mesures de sécurité.	Renforcement de la supervision et des capacités d'audit pour assurer une application efficace des mesures de sécurité.
Coopération et partage d'information	Coopération volontaire et ad hoc entre États membres.	Renforcement des structures de coopération, avec des obligations claires pour le partage d'informations.
Rôle des CSIRT	Les CSIRT fonctionnent avec des capacités variables selon les États.	Renforcement et collaboration accrue des CSIRT nationaux pour une réponse coordonnée aux incidents.

Tableau 5: Tableau comparatif directive NIS 1 et NIS 2

2.7.6 Scope

Comme expliqué plusieurs fois, le champ d'application de la directive NIS 2 a été considérablement élargi par rapport à celui de la directive NIS 1 et n'est plus nécessairement lié à l'identification préalable des entités concernées par les autorités nationales compétentes.

Essentiellement, une entité est couverte par le champ d'application si elle :

- Opère dans l'un des (sous-)secteurs et types de services énumérés dans les annexes de la directive,
- Est d'une certaine taille.

Figure 25: NIS 2 scope – Final version

CCB. (2024-c, 9 avril). *La directive NIS2 : que cela signifie-il pour mon organisation ?* Consulté le 19 avril 2024, à l'adresse https://ccb.belgium.be/fr/la-directive-nis2-que-cela-signifie-il-pour-mon-organisation

Après ma discussion avec le Head of Legal du CCB Valery Vanden Geeten (2024), ainsi qu'un article publié par eux sur leur site expliquant quelles sont les entités qui sont dans le scope ou pas j'en retiens que, sauf exception, il n'y a plus d'identification active dans le NIS 2. Une entité opérant dans les secteurs énumérés ci-dessus entre dans le champ d'application s'il s'agit d'une grande ou moyenne entreprise. C'est-à-dire qu'elle emploie plus de 50 personnes ou réalise un chiffre d'affaires annuel supérieur à 10 millions d'euros. Pour les petites et microentreprises, moins de 50 salariés et un chiffre d'affaires annuel (ou un total de bilan annuel) inférieur à 10 millions d'euros - conditions cumulatives) sont exclus du champ d'application de la directive, sauf exception.

L'ancienne distinction entre "opérateurs de services essentiels" (OES) et "fournisseurs de services numériques" (FSN) disparaît et est remplacée par une distinction entre entités "essentielles" et "importantes". Cette distinction est faite automatiquement en fonction de la taille de l'entité et du type d'entité concernée. La différence entre les entités essentielles et les entités importantes réside principalement dans la rigueur de la surveillance et des sanctions. Les entités essentielles feront l'objet d'un contrôle et de sanctions plus stricts que les entités importantes. Les entités essentielles sont de grandes entreprises qui font partie des secteurs de haute criticité énumérés à l'annexe I de la directive. Une grande entité est définie comme une entreprise employant au moins 250 personnes ou ayant un chiffre d'affaires annuel d'au moins 50 millions d'euros ou un total de bilan annuel d'au moins 43 millions d'euros.

Les entités importantes sont des entreprises moyennes opérant dans les secteurs de haute criticité de l'annexe I de la directive, ou des grandes ou moyennes entreprises dans les secteurs de l'annexe II de la directive qui n'entrent pas dans la catégorie des entités essentielles (en raison de leur taille ou du type d'entité impliquée). Une entreprise moyenne est définie comme une entreprise employant au moins 50 personnes ou dont le chiffre d'affaires annuel (ou le total du bilan) est d'au moins 10 millions d'euros, mais qui emploie moins de 250 personnes ET dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros ou le total du bilan n'excède pas 43 millions d'euros.

Il existe toutefois quelques exceptions. Dans certains secteurs, des entités, quelle que soit leur taille, sont désignées comme "essentielles", par exemple les fournisseurs de réseaux publics de communications électroniques, les entités désignées comme critiques au niveau national en vertu du règlement d'exemption par catégorie, les services gouvernementaux (au niveau central), les fournisseurs de services de confiance qualifiés et les registres de noms de domaine de premier niveau et les fournisseurs de services DNS. Outre ces règles, les autorités nationales peuvent également désigner spécifiquement des entités comme "essentielles" ou "importantes", par exemple lorsqu'elles sont le seul fournisseur de services ou lorsqu'une interruption de la fourniture de services pourrait avoir des conséquences importantes pour la sécurité publique, la sûreté publique ou la santé publique.

L'ensemble de ces éléments constitue un système de portée assez complexe. Il est toutefois important de rappeler qu'il ne s'agit que des règles d'harmonisation minimale européenne. Dans la législation belge de transposition, des spécifications supplémentaires ou plus strictes peuvent être introduites. (CCB, 2024-c).

2.7.7 Les différents articles

Au cœur de la directive NIS 2 réside le concept de conformité, impératif pour les organisations s'efforçant d'assurer une gestion sécurisée de leurs systèmes d'information. Cette conformité dépasse le simple cadre de l'obligation légale pour devenir une nécessité stratégique. En ciblant les opérateurs d'infrastructures critiques ainsi que les fournisseurs de services numériques, la directive vise à garantir la résilience des infrastructures face aux cyberattaques et à sécuriser les services offerts aux utilisateurs. De plus, en encourageant la coopération entre les États membres de l'UE, la directive favorise une collaboration renforcée en matière de cybersécurité à l'échelle européenne.

Après avoir examiné les considérants de la directive NIS 2, qui posent les fondations et le contexte de cette législation, et expliqué la transition vers celle-ci, il est essentiel de se pencher sur les articles spécifiques de la directive pour comprendre les obligations légales précises et les mesures de conformité requises. Les articles définissent les responsabilités concrètes des entités concernées, les exigences en matière de sécurité et les protocoles de notification des incidents, ainsi que les modalités de supervision et d'application par les autorités nationales. Ces dispositions constituent le cœur opérationnel de la directive, transformant les principes énoncés dans les considérants en actions et procédures pratiques que doivent suivre les entités régulées.

Pour l'analyse détaillée des articles, il est crucial de comprendre comment ces exigences interagissent avec les réalités opérationnelles des organisations concernées. Chaque article apporte une pierre à l'édifice de la cybersécurité européenne, contribuant à une infrastructure plus sûre et plus résiliente. En explorant ces articles, nous mettrons en lumière les mécanismes spécifiques par lesquels la directive

NIS 2 cherche à renforcer la sécurité des réseaux et des systèmes d'information à travers l'Union européenne, et comment les organisations peuvent et doivent adapter leurs pratiques pour se conformer à ces nouvelles réglementations. Ce passage des principes aux pratiques est essentiel pour toute organisation cherchant à naviguer efficacement dans le paysage de la cybersécurité réglementée par l'UE.

Je vais analyser le chapitre 4 du texte de loi, et principalement les articles 20, 21 et 23, car c'est là que se trouve le cœur même de la directive. C'est dans ces articles que sont énoncées les obligations des entreprises en matière de sécurité des réseaux et des systèmes d'information.

2.7.7.1 Article 20 : gouvernance

L'article 20 de la directive NIS 2 aborde la responsabilité et la formation en matière de cybersécurité au sein des entités jugées essentielles et importantes pour les infrastructures et les services européens. (Parlement européen et Conseil de l'Union européenne, 2022).

Responsabilité des organes de direction :
Les États membres doivent s'assurer que les cadres dirigeants (par exemple, les membres du conseil d'administration) des entités essentielles et importantes sont activement impliqués dans la cybersécurité. Ces dirigeants doivent approuver les politiques et procédures de gestion des risques de cybersécurité, superviser leur mise en œuvre, et être légalement responsables en cas de non-conformité avec les exigences de la directive, sauf si le droit national spécifie autrement en ce qui concerne la responsabilité publique.

Formation des organes de direction et des employés :
Les États membres doivent aussi veiller à ce que les dirigeants de ces entités reçoivent une formation pour comprendre et gérer les risques de cybersécurité.
Ils encouragent les entités à fournir régulièrement des formations similaires à leurs employés pour s'assurer qu'ils ont les connaissances et les compétences nécessaires pour identifier les risques de cybersécurité et évaluer l'impact de ces risques sur les services de l'entité.

On parle donc de l’implication du top management qui est un domaine important de la directive. Cela implique donc un engagement à haut niveau. Les hauts responsables ne peuvent pas se désengager des questions de cybersécurité. Ils doivent s'impliquer directement dans la prise de décision et la supervision des pratiques de cybersécurité de l'entité. La direction peut être tenue responsable si l'entité ne respecte pas les règles de sécurité établies dans l'article 21, ce qui signifie qu'il y a une pression juridique pour que les pratiques de cybersécurité soient prises au sérieux.
La directive reconnaît que la gestion des risques de cybersécurité n'est pas seulement une question technique, mais aussi une question de compétence et de conscience à tous les niveaux de l'organisation. Cela encourage le développement d'une culture organisationnelle où la cybersécurité est intégrée dans la routine quotidienne et la formation continue du personnel.

2.7.7.2 Article 21 : Mesures de gestion des risques liés à la cybersécurité

L'article 21 de la directive NIS 2 établit les obligations des entités essentielles et importantes en matière de mesures de cybersécurité.

D’abord les États membres doivent garantir que les entités essentielles et importantes prennent des mesures techniques, opérationnelles et organisationnelles adéquates pour gérer les risques de sécurité de leurs réseaux et systèmes informatiques.
Ces mesures doivent être proportionnelles au niveau de risque, en prenant en compte l'état de l'art, les normes européennes et internationales pertinentes, ainsi que les coûts d'implémentation.
L'évaluation des mesures de sécurité doit considérer la taille de l'entité, la probabilité et la gravité des incidents possibles, et leur impact économique et social.
Ceci implique que les entités doivent prendre en main leur cybersécurité et mettre en œuvre des mesures qui correspondent à leur niveau de risque spécifique.

Les entités se doivent de gérer les risques inhérents à la sécurité de leurs réseaux et systèmes d'information, qui sont vitaux pour leurs activités opérationnelles et la prestation de leurs services. La prévention et la réduction de l'impact des incidents de cybersécurité ne sont pas seulement essentielles pour la continuité des activités de ces entités, mais aussi pour protéger les utilisateurs de leurs services ainsi que la viabilité d'autres services qui pourraient être affectés.

Les organes de direction des entités essentielles et importantes devront approuver les mesures de gestion des risques en matière de cybersécurité, superviser leur mise en œuvre et pourront être tenus responsables des éventuels manquements.

Ensuite vient la notion d’approche tous risques. Les mesures de sécurité doivent être fondées sur une approche tous risques, c’est-à-dire qu'elles doivent couvrir toutes les menaces potentielles et protéger à la fois les systèmes informatiques et leur environnement physique. Que ce soit une simple panne d’électricité à un tsunami ou une attaque d’un autre état, le système doit être fondé pour permettre de réagir à toute éventualité et à y faire face. En fonction du scénario cela va changer, mais toujours est-il qu’il faut être prêt. Il est cherché ici à ce que les entités aient une approche proactive.

Les mesures de sécurité :

(a) des politiques d'analyse des risques et de sécurité des systèmes d'information.
(b) La gestion des incidents.
(c) La continuité des affaires, y compris la gestion des sauvegardes, la récupération après sinistre et la gestion de crise.
(d) La sécurité de la chaîne d'approvisionnement.
(e) La sécurité lors de l'acquisition, du développement et de la maintenance des systèmes.
(f) Des procédures pour évaluer l'efficacité des mesures de gestion des risques de cybersécurité.
(g) Des pratiques de base en matière de cyberhygiène et des formations en cybersécurité.
(h) L'utilisation de la cryptographie et de l'encryption.
(i) La sécurité des ressources humaines, les politiques de contrôle d'accès et la gestion des actifs.
(j) L'utilisation de l'authentification multifacteur ou de solutions d'authentification continue, ainsi que des communications sécurisées.

Ces mesures de sécurité forment un cadre complet pour la cybersécurité des entités essentielles et importantes, abordant de manière proactive les multiples facettes des risques numériques. L'intérêt de ces mesures est d'établir un niveau élevé de sécurité qui est essentiel pour maintenir la confiance dans le marché intérieur et pour protéger l'infrastructure critique de l'Union européenne. L’objectif est de via des Frameworks respecter chacune de ses mesures et être sûr que les entités ont mis en place les actions nécessaires pour répondre à chacune de ces mesures.

L'intérêt derrière le choix de ces mesures est de créer un système de sécurité à plusieurs niveaux qui soient difficiles à pénétrer et qui puissent résister à une variété d'attaques, tout en assurant une gestion efficace et une résilience en cas d'incident. En intégrant ces diverses mesures, les entités visent à minimiser les risques de cybersécurité et à maximiser leur capacité à opérer de manière sûre et sécurisée, protégeant ainsi les services essentiels qu'elles fournissent et l'économie dans son ensemble. (Parlement européen et Conseil de l'Union européenne, 2022).

2.7.7.3 Article 23 : Obligation de déclarations

Sous NIS2, chaque État membre maintient un point de contact central et une équipe CSIRT pour la conformité et le rapportage des incidents de cybersécurité, le CCB jouant ce rôle en Belgique. Une équipe CSIRT désigne une équipe ou une organisation chargée de recevoir, d'analyser et de répondre aux notifications et activités concernant la sécurité informatique, notamment les incidents de sécurité et les vulnérabilités. (Scheelen et al., 2023)

L'article 23 énonce les obligations de notification en cas d'incidents significatifs liés à la sécurité des réseaux et des systèmes d'information. Les entités essentielles et importantes doivent informer sans délai leurs CSIRT (Computer Security Incident Response Team) ou l'autorité compétente de tout incident susceptible d'avoir un impact important sur la fourniture de leurs services. Elles doivent également notifier les destinataires de leurs services des incidents significatifs susceptibles de perturber la fourniture de ces services. Les États membres doivent veiller à ce que les entités fournissent toutes les informations nécessaires pour évaluer l'impact transfrontalier de l'incident. Les entités concernées doivent soumettre des rapports initiaux, intermédiaires et finaux sur les incidents, décrivant en détail la nature de l'incident, ses causes, les mesures d'atténuation et, le cas échéant, son impact transfrontalier. Les CSIRT ou l'autorité compétente doivent répondre rapidement aux notifications, fournir des conseils opérationnels et, si nécessaire, orienter vers les autorités judiciaires en cas de suspicion d'activité criminelle.

Le CCB qui prend ce rôle via le service qu'ils ont créé nommé CERT. Les entités essentielles et importantes devront notifier, sans retard injustifié, tout incident ayant un impact significatif sur la fourniture des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la directive.

Un incident significatif est un incident qui :

1° soit a causé ou est susceptible de causer une perturbation opérationnelle grave des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la directive ou des pertes financières pour l'entité concernée ; ou

2° a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

La notification pourra comprendre différentes étapes comme indiqué dans la figure ci-dessous :

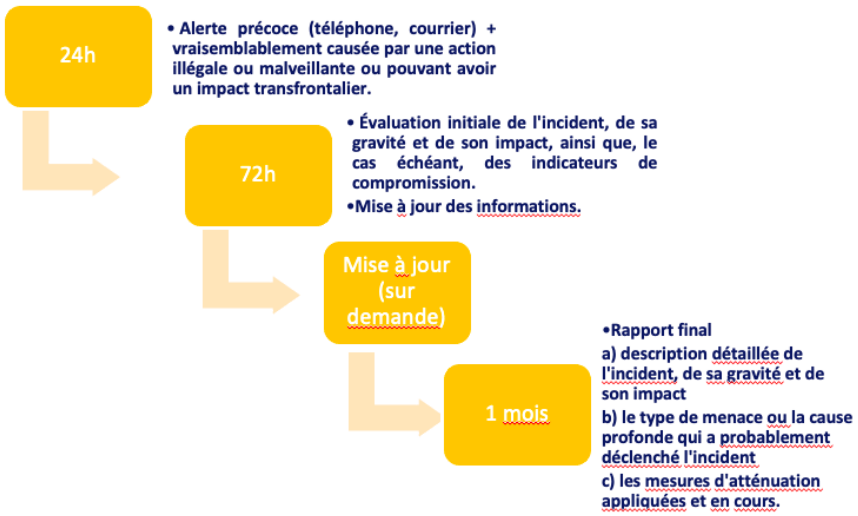


Figure 26: Notification d'incident
Source : CCB. (2023, juin) *NIS 2 in BE* [Présentation Power Point]. CCB

En effet, la directive NIS 2 établit des exigences strictes en matière de notification des incidents pour les entités couvertes. Lorsqu'un incident a un impact significatif sur les réseaux et systèmes d'information d'une entité ou affecte les utilisateurs de ses services, causant un dommage matériel, corporel ou moral considérable, l'entité est tenue de le notifier. Cette obligation s'étend aux incidents susceptibles de menacer les droits et libertés des individus. Une alerte précoce doit être communiquée au CERT national ou à l'autorité compétente dans les plus brefs délais, idéalement dans les 24 heures suivant la découverte de l'incident, pour permettre une réponse rapide et coordonnée. En outre, une notification complète de l'incident est requise dans les 72 heures. Cette rapidité de communication est parallèle à celle exigée pour la notification à l'Autorité de Protection des Données (APD), qui doit aussi être informée dans les meilleurs délais et, si possible, sous 72 heures après la connaissance de l'incident. Cette coordination des notifications vise à assurer une gestion transparente et efficace des incidents de cybersécurité, soulignant la nécessité d'une réponse rapide pour atténuer les risques et les dommages potentiels. (Lexing, 2023)

Ce nouveau processus de notification exige donc que les incidents significatifs soient signalés immédiatement, avec un avertissement précoce sous 24 heures et un rapport détaillé sous 72 heures, décrivant l'incident, sa gravité, son impact et les preuves de compromission. Un rapport final doit être fourni dans le mois suivant l'incident.

2.7.8 Supervision

Les amendes et sanctions pour non-conformité sont désormais du ressort des autorités compétentes. Les entités auront pour obligation de notifier sans retard injustifié, aux autorités nationales compétentes (notamment le CSIRT national – en Belgique le CCB) tout incident ayant un impact significatif sur la fourniture des services fournis dans les secteurs. Un incident est ce qui :
1° soit a causé ou est susceptible de causer une perturbation opérationnelle grave des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la directive ou des pertes financières pour l'entité concernée ; ou

2° a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

En cas de non-respect les entités peuvent être sanctionnées lourdement. Selon chaque état membre, l'autorité nationale aura le pouvoir de décider ce qu'elle veut mettre en place pour contrôler les entités, que ce soit la réalisation d'audits externes réguliers, effectuer des inspections ou solliciter la production de certains documents. Les autorités pourront notamment émettre des avertissements ou des instructions contraignantes afin de remédier aux insuffisances constatées ou encore d'informer leurs clients. En complément de ces mesures administratives, des amendes administratives effectives, proportionnées et dissuasives pourront être également imposées. (CCB, 2024-c).

Ainsi, les violations en matière de mesures de gestion des risques ou de notification d'incident pourront être punies :

- Pour les entités essentielles à des amendes administratives d'un montant maximal s'élevant à au moins 10 000 000 EUR ou à au moins 2% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu ;
- Pour les entités importantes à des amendes administratives d'un montant maximal s'élevant à au moins 7 000 000 EUR ou à au moins 1,4% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu.

La supervision "ex ante" et "ex post" sont deux approches réglementaires clés utilisées dans le cadre de cette directive pour assurer le respect des normes de cybersécurité.
La supervision "ex ante" fait référence à des mesures préventives et à des évaluations de sécurité qui sont effectuées avant qu'un incident ne se produise. La supervision "ex post", quant à elle, intervient après qu'un incident de sécurité a eu lieu. Elle comprend des activités telles que des enquêtes sur les incidents, des analyses de la cause profonde, et l'évaluation de la réponse de l'entité à l'incident. Cette forme de supervision permet aux régulateurs de vérifier que les entités ont adéquatement répondu à l'incident et de prendre des mesures correctives si nécessaire. Elle aide également à tirer des leçons des incidents pour améliorer la résilience globale du système.
Les entités essentielles seront soumises à une supervision ex ante et ex post, tandis que les entités importantes seront tenues à une supervision ex post. (Vanden Geeten, 2024).

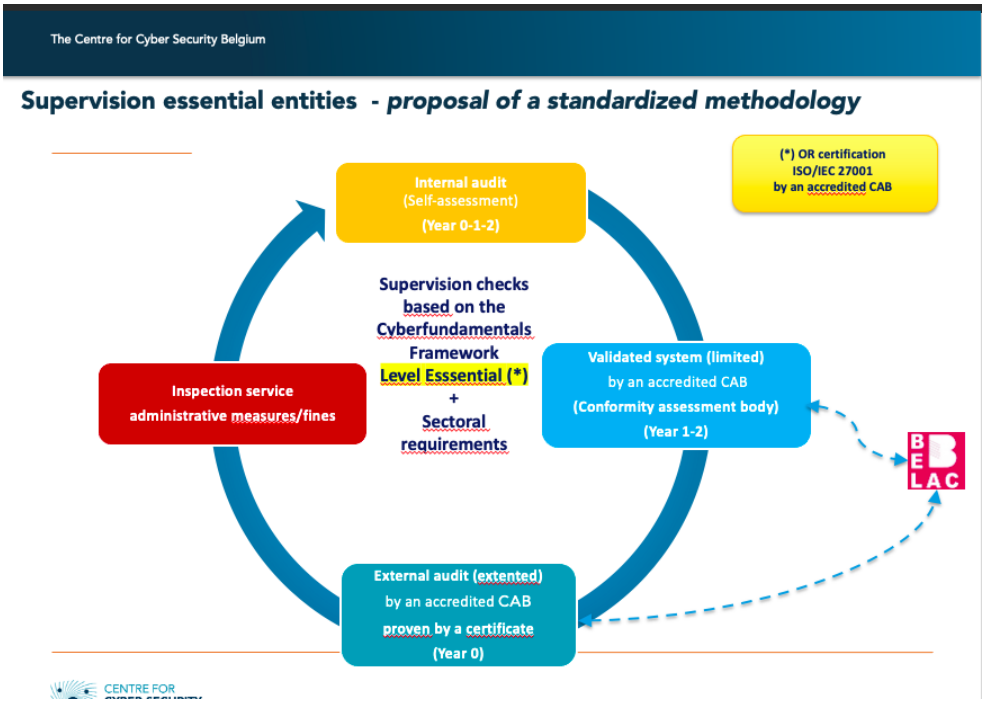


Figure 27: Supervision des entités essentielles
CCB. (2023, juin) *NIS 2 in BE* [Présentation Power Point]. CCB

1. **Audit interne (Auto-évaluation) (Année 0-1-2)** :
    - Cette phase est la première étape où l'entité réalise une auto-évaluation de sa cybersécurité. Cela peut inclure une revue interne des politiques, des processus, des contrôles et de la gestion des risques en place. C'est une vérification de conformité avec les normes internes et le cadre réglementaire applicable, comme la norme ISO/IEC 27001, qui est un standard international pour la gestion de la sécurité de l'information.
2. **Système validé (limité) par un organisme d'accréditation CAB (Organisme d'évaluation de la conformité) (Année 1-2)** :
    - Après les vérifications initiales, le système de l'entité est évalué par un organisme d'évaluation de la conformité (CAB) accrédité, pour garantir que la mise en œuvre des contrôles de cybersécurité est conforme aux exigences normatives et sectorielles. Cette validation peut être limitée dans le sens où elle ne couvre pas nécessairement tous les aspects du système de gestion de la sécurité de l'information de l'entité, mais se concentre sur des aspects clés.
3. **Audit externe (étendu) par un CAB accrédité, prouvé par un certificat (Année 0)** :
    - Ici, un audit externe est réalisé par un CAB accrédité. Cet audit est plus approfondi que l'auto-évaluation et vise à fournir une certification formelle de conformité avec les normes de cybersécurité, telles que l'ISO/IEC 27001. Le résultat est une attestation officielle de conformité.
4. **Service d'inspection + mesures administratives/amendes** :
    - Dans cette dernière phase du cycle, un service d'inspection vérifie les résultats de l'audit et les mesures de sécurité mises en place. Si des lacunes sont identifiées, ou si l'entité ne répond pas aux normes requises, des mesures administratives peuvent être imposées, y compris des amendes.

2.7.9 Framework

Pour mettre en place ces mesures imposées par la directive, que ce soit au niveau de la gouvernance, des infrastructures ou autres, un framework est un outil essentiel pour structurer tout cela, surtout lors de l'adaptation aux exigences de la directive NIS 2. Ces ensembles de lignes directrices méthodiquement organisées fournissent une démarche standardisée qui permet de sécuriser les systèmes d'information de manière vérifiée et efficace, un avantage non négligeable vu la complexité technique de la cybersécurité.

L'intégration d'un tel cadre garantit une couverture exhaustive des risques de sécurité, assurant l'inclusion de toutes les précautions essentielles et l'alignement des politiques de sécurité avec les objectifs et obligations commerciales, légales et réglementaires.

Pour la directive NIS 2, plusieurs frameworks de cybersécurité sont reconnus et peuvent être appliqués. Par exemple :

1) ISO/IEC 27001 : Il s'agit d'une norme internationale qui fournit des exigences pour les systèmes de gestion de la sécurité de l'information (SGSI). Elle aide les organisations à évaluer le risque et à mettre en place des mesures de sécurité adéquates.
2) CyberFundamentals est un framework créé par le centre pour la cybersécurité en Belgique (CCB) et qui a pour but de donner un ensemble de mesures concrètes visant à protéger les données et réduire de manière significative le risque des cyberattaques les plus courantes ainsi qu'accroitre la cyberrésilience d'une organisation.
3) Self assessment : qui est une méthodologie où l'entreprise décide par elle-même d'utiliser sa propre manière de faire et elle se fera inspecter par le service du CCB. Mais il y a une correspondance à faire au préalable et un mapping sur comment ils ont mis cela en place. (entretien CCB)

Il y a un peu des différences méthodologiques entre chaque framework, ISO 27001 est basée sur aller faire une analyse des risques détaillés, donc ça prend plus de temps et plus d'énergie. Par contre c'est plus destiné pour de toutes grosses boîtes ou bien pour des multinationales. C'est un truc qu'ils connaissent assez facilement, mais ça implique plus de travail parce qu'il faut vraiment identifier tous les risques et aller l'analyser.
L'autre solution, qui est plus simple, c'est d'appliquer le CYFUN. Il inclut déjà une sorte d'analyse de risque. En fait, il fait déjà un catalogue de tous les risques principaux qui doivent être couverts.
C'est vraiment l'entreprise qui doit choisir ce qui lui correspond le mieux. Soit elle a déjà des processus en place et c'est plus simple, soit elle est plus habituée à ISO 27001, soit elle veut vraiment le package déjà tout fait et elle prend le CYFUN.

Ces frameworks ne sont pas exclusifs et peuvent souvent être utilisés conjointement pour renforcer l'approche globale de la cybersécurité d'une organisation. Dans le cadre de mon plan d'action, je vais me concentrer sur le CyberFundamentals pour la mise en place des mesures de la directive.

2.7.9.1 CyberFundamentals

Le CCB a lancé un ensemble de lignes directrices visant à garantir et à améliorer en permanence la cybersécurité dans les secteurs public et privé. Cette initiative ainsi que tous les investissements déployés ont permis de classer la Belgique dans de nombreux classements internationaux comme pays majeurs en matière de cybersécurité.

Les Cyberfundamentals sont structurés selon quatre niveaux, contenant chacun un peu plus de mesures que le précédent. Le premier niveau est SMALL, suivi de BASIC, IMPORTANT et ESSENTIAL. L'objectif est qu'à terme, chaque PME et chaque organisation de notre pays atteigne le niveau BASIC. Le Cyberfundamentals Framework s'articule autour de cinq fonctions essentielles : identifier, protéger, détecter, répondre et récupérer. Ces fonctions favorisent la communication autour de la cybersécurité entre les experts du domaine et les parties prenantes, afin que les risques liés à la cybersécurité puissent être intégrés dans la stratégie globale de gestion des risques des organisations. Il permet également d'accroître la résilience des entreprises face aux cyberattaques.

Le cadre est basé et s'inspire sur quatre cadres de cybersécurité couramment utilisés, auxquels il est lié NIST CSF, ISO 27001 / ISO 27002, CIS Controls et IEC 62443. L'idée derrière est de tirer le meilleur de tous les mondes pour en faire un framework le plus complet. L'objectif derrière est de rendre la Belgique comme pays le moins vulnérables. Il va m'aider ici à répondre aux mesures pour la directive NIS 2, mais il ne se limite pas à cela. (CCB, 2023)

Les différents niveaux de ce framework vont permettre aux entreprises petites ou grandes qui veulent se conformer d'aller petit à petit, car pour la plupart des entreprises, leurs maturités sont faibles et il est très difficile de demander d'avoir énormément de mesures et contrôles d'un coup.

Le niveau de départ Small est la base de protection, les mesures qui y sont indiquées sont assez simples. Il permet à une organisation de procéder à une première évaluation. Il est destiné aux micro-organisations ou aux organisations ayant des connaissances techniques limitées. Ensuite, le niveau d'assurance Basic, avec 34 contrôles, contient les mesures de sécurité de l'information standard pour toutes les entreprises. Ceux-ci fournissent une valeur de sécurité efficace avec des technologies et des processus qui sont généralement déjà disponibles. Lorsque cela se justifie, les mesures sont adaptées et affinées. Pour le niveau d'assurance Important, et ses 107 contrôles, il a été conçu pour minimiser les risques de cyberattaques ciblées par des acteurs disposant de compétences et de ressources communes, en plus des risques de cybersécurité connus. Enfin, le niveau d'assurance essentiel, avec ses 144 contrôles, va plus loin et est conçu pour faire face au risque de cyberattaques avancées par des acteurs disposant de compétences et de ressources étendues. (CyberFundamentals Framework | CCB SafeOnWeb, s. d.)

Sur la base des données historiques du CCB, un rétrofit a été effectué sur les cyberattaques réussies en utilisant des données anonymes. La conclusion est la suivante :

- Les mesures du niveau d'assurance Basic sont capables de couvrir 82% des attaques,
- Les mesures du niveau d'assurance Important permettent de couvrir 94 % des attaques,
- Les mesures du niveau d'assurance essentiel sont capables de couvrir 100 % des attaques.

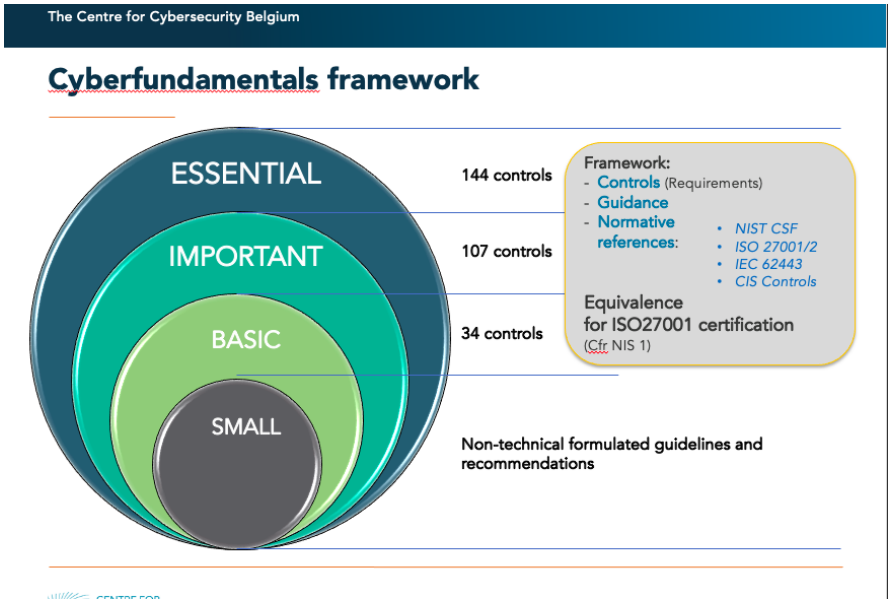


Figure 28: Différent niveau du Framework
CCB. (2023, juin) *NIS 2 in BE* [Présentation Power Point]. CCB

2.7.10 Certification

J'ai mené un entretien avec un expert en législation qui s'occupait de la proposition de la transposition de la directive NIS 2 -en Belgique. Cette personne m'a expliqué comment se passait le processus de certification.
Selon lui, les entités classées comme essentielles ont des obligations de conformité plus strictes en raison de leur impact potentiel sur la sécurité nationale, la santé économique, et la sûreté publique. Ces entités doivent, effectuer une évaluation annuelle de conformité, vérifier par un auditeur externe. Cette évaluation peut s'aligner sur des standards reconnus tels qu'ISO 27001 ou Cyber Fundamental (CYFUN), garantissant ainsi une approche standardisée et rigoureuse à la gestion des risques de sécurité. Elles doivent également utiliser des certifications comme Cyber Fundamental ou ISO 27001 qui sont validées par des auditeurs externes, fournissant une preuve tangible de leur diligence en matière de cybersécurité.
Pour les entités importantes, la certification est encouragée, mais n'est pas mandatée. Cependant, elles restent sujettes à des inspections ponctuelles, surtout en réaction à des incidents ou des manquements rapportés.
Ces entités peuvent choisir de se conformer volontairement aux standards de certification pour démontrer proactivement leur engagement envers la cybersécurité.
En l'absence d'obligation, l'inspection par les services réglementaires se fait généralement a posteriori, c'est-à-dire après un incident signalé.

Les entités peuvent choisir parmi plusieurs méthodologies de certification basées sur leurs besoins spécifiques, leur familiarité avec les cadres de conformité existants, ou leurs ressources internes :

1. **ISO 27001** : Favorisé par de grandes entreprises ou multinationales, ce standard requiert une analyse de risque détaillée et un engagement continu en matière de gestion de la sécurité de l'information.
2. **CYFUN** : Offre une approche simplifiée, idéale pour les entreprises cherchant un cadre structuré, mais moins onéreux en termes de temps et d'effort. CYFUN intègre une analyse préétablie des risques, facilitant ainsi l'adoption pour les petites et moyennes entreprises.

3. **Approches Propres** : Les entreprises peuvent également opter pour des méthodes personnalisées de gestion de la cybersécurité. Dans ce cas, elles doivent démontrer la conformité de leurs pratiques à travers un "mapping" avec des cadres reconnus comme ISO ou CYFUN.

Les organismes de certification (CAB) jouent un rôle crucial dans le processus de validation de la conformité. Ils sont responsables de :

- Évaluer les entités selon les critères établis par les cadres de certification choisis.
- Délivrer des certifications qui attestent de la conformité de l'entité.
- Être régulièrement inspectés eux-mêmes pour s'assurer de leur intégrité et de la rigueur de leurs pratiques d'évaluation.

La mise en œuvre de la directive NIS 2 exige une attention particulière aux processus de certification pour les entités essentielles et importantes. Bien que les entités essentielles soient soumises à des exigences de certification strictes, les entités importantes bénéficient d'une flexibilité qui leur permet d'adapter leur approche à la certification. L'adoption de cadres comme ISO 27001 ou CYFUN peut aider toutes les entités à structurer efficacement leur gestion de la cybersécurité, tout en offrant la possibilité de démontrer leur conformité de manière vérifiable et reconnue au niveau européen.

2.8 Conclusion intermédiaire

Vous l'aurez compris, nous vivons dans une société où les menaces sont de plus en plus présentes avec des technologies beaucoup plus développées. L'émergence de réglementations comme le RGPD et les directives NIS sont là pour encadrer et mettre en place des mesures de sécurité nécessaires pour protéger les infrastructures critiques contre ces menaces croissantes.

Dans cette section, j'ai pu présenter et analyser différents aspects théoriques liés à la sécurité des systèmes d'information, les cybermenaces, les technologies émergentes et la gestion des risques et des incidents. L'importance de la sécurité de l'information dans les organisations a été soulignée, et des cadres référentiels ont été présenté.

L'évolution rapide des technologies numériques a augmenté la surface d'attaque et les menaces sont devenues plus complexes et fréquentes, nécessitant une réponse réglementaire plus robuste. La directive NIS 2 vise à renforcer cette réponse en couvrant davantage de secteurs essentiels et en unifiant les critères d'identification des opérateurs de services essentiels et fournisseurs de services numériques pour une meilleure clarté juridique.

Nous devons maintenant nous demander comment faire parvenir ces informations aux entreprises et les sensibiliser aux enjeux de la cybersécurité. Sont-elles conscientes des défis auxquels nous faisons face et ont-elles une approche proactive à l'approche de la transposition de la directive en Belgique ? Malheureusement, rares sont les entreprises aujourd'hui qui sont réellement "cyber résilientes". Cependant, avec cette nouvelle directive, les sanctions qui l'accompagnent et une conscientisation émergente des entités, sommes-nous sur la bonne voie de la cyber résilience ?

La prochaine section mettra en avant les initiatives en place pour justement accompagner et conscientiser ces acteurs. Nous verrons pourquoi il est important de promouvoir cela et quelles sont les solutions qu'Agoria envisage pour y remédier.

Section 3 : Plan d’action : Étude de cas Agoria

3.1 Introduction

La promotion de la cybersécurité en Belgique est un aspect crucial dans le contexte de la mise en œuvre de la directive NIS 2. Dans cette section, je présente les efforts déployés par Agoria pour promouvoir la cybersécurité, ainsi que d'autres initiatives visant à sensibiliser, former et accompagner les entreprises belges dans leur démarche de sécurité informatique.

Agoria, en tant que fédération sectorielle de l'industrie technologique belge, joue un rôle clé dans la promotion de la cybersécurité et de la directive NIS 2. À travers diverses actions et programmes, Agoria s'efforce de sensibiliser les entreprises aux enjeux de la cybersécurité, de fournir des formations spécialisées et de proposer des conseils stratégiques pour assurer une mise en conformité efficace. Parmi ces initiatives, on retrouve des campagnes de sensibilisation, des ateliers de formation, des publications de guides pratiques, et l'organisation de forums de discussion entre professionnels du secteur.

L'objectif de cette section est double. Premièrement, après avoir présenté les concepts théoriques et l'analyse exploratoire sur la cybersécurité et la directive NIS 2, il s'agit de montrer comment ces théories se traduisent sur le terrain. Deuxièmement, il est essentiel de démontrer comment les missions et les initiatives d'Agoria contribuent à diffuser le message de l'importance de la cybersécurité et à encourager les entreprises à adopter des mesures de sécurité robustes.

Ainsi, au cours de ce chapitre, je vais détailler les différentes actions mises en place par Agoria auxquelles j’ai pu participer et contribuer, telles que les programmes de formation, les outils de communication et les ressources disponibles pour les entreprises. En explorant ces initiatives, je vais illustrer comment Agoria soutient les entreprises dans leur transition vers la conformité à la directive NIS 2 et renforce la résilience cybernétique globale en Belgique.

3.2 Promotion de la cybersécurité en Belgique

La promotion de la cybersécurité en Belgique est un aspect crucial dans le contexte de la mise en œuvre de la directive NIS 2. Dans cette section, je présente les efforts déployés par Agoria pour promouvoir cela ainsi que d'autres initiatives, pour sensibiliser, former et accompagner les entreprises belges dans leur démarche de sécurité informatique.

3.2.1 Agoria et NIS 2

Comme expliqué Agoria est la fédération de la technologie en Belgique. Agoria y joue un rôle essentiel en tant qu'organisation représentative des entreprises du secteur. Son rôle comprend plusieurs aspects. Elle va notamment représenter les intérêts du secteur, Agoria représente les intérêts des entreprises technologiques belges auprès des décideurs politiques nationaux et internationaux. Son objectif est de promouvoir un environnement favorable à la croissance et à l'innovation pour les entreprises du secteur. Agoria encourage la collaboration et le réseautage entre les entreprises technologiques, les institutions

académiques et les autorités publiques. Cela permet de stimuler l'innovation et le partage des meilleures pratiques. La fourniture de services et de conseils est aussi une des missions d'Agoria. Elle offre une gamme de services et de conseils aux entreprises membres, notamment en matière de réglementation, de normes, de technologies émergentes et de développement des affaires. Elle joue donc un rôle de catalyseur pour l'innovation et le développement technologique. Pour ce qui est des entreprises avec des intérêts cyber, elle possède une centaine de membres. (Van Cangh, 2024)

Dans le cadre de la mise en œuvre de la Directive NIS 2, une stratégie de communication approfondie est en cours d'élaboration pour sensibiliser et informer les entités concernées. Cette stratégie comprend la diffusion de fiches d'informations et de brochures explicatives, visant à clarifier des éléments clés tels que le champ d'application de la directive, les exigences de notification des incidents, et d'autres aspects pertinents. Des initiatives telles que la NIS Academy reçoivent un soutien appuyé, dans le but d'enrichir la compréhension et la conformité à la directive. La mise à disposition d'une foire aux questions détaillée, destinée à être publiée en ligne, fait partie intégrante de cette démarche éducative.

Il est à noter que la finalisation de certains textes législatifs est un préalable indispensable à cette démarche de communication. Toute campagne informative doit s'appuyer sur des bases juridiques stables et officiellement adoptées. Par conséquent, bien que la stratégie de communication soit déjà bien avancée avec l'élaboration d'un plan et la préparation de divers matériaux informatifs, la diffusion active de ces ressources n'aura lieu qu'après l'adoption définitive et la validation des textes en question. Cette phase active de communication est prévue pour se déployer jusqu'en octobre de l'année en cours, et se prolongera au-delà pour assurer une compréhension complète et précise de la Directive. (Vanden Geeten, 2024)

Selon Eric Van Cangh (2024) et Valery Vanden Geeten (2024), durant l'année écoulée, une série de groupes de travail a été mise en place pour élaborer la mise en œuvre de la Directive NIS 2. Ces groupes ont rassemblé une diversité d'acteurs, incluant les administrations publiques, le secteur privé, ainsi que diverses associations et organisations telles qu'Agoria, Beltug, la Cyber Security Coalition et la FEB. Ces rencontres ont favorisé la réflexion collaborative, aboutissant à des ébauches et des propositions préliminaires. Les débats ont porté sur la manière la plus adéquate d'appliquer les exigences de la directive, les outils à développer pour faciliter cette mise en œuvre et l'intégration des perspectives de chaque partie prenante afin de minimiser les différences entre les États membres, comme observés lors de l'évaluation de NIS 1.

En parallèle, une consultation publique a été organisée autour du projet de loi et de l'arrêté royal, dans le but de recueillir une pluralité d'avis et de suggestions. Bien que la décision finale relève du pouvoir politique — le Parlement et les autorités compétentes —, ces derniers reposent sur des conseils et propositions élaborées. Il est essentiel de présenter des recommandations concrètes, élaborées à partir d'un consensus éclairé par les contributions de divers intervenants, tout en reconnaissant qu'il est impossible de consulter chaque acteur individuellement.

Les entreprises, conscientes du risque cybernétique, comprennent la nécessité d'augmenter leurs standards de cybersécurité. Cependant, elles expriment des inquiétudes quant à la charge que cela représente pour leurs opérations et leur compétitivité. En réponse, les stratégies proposées cherchent à équilibrer la protection contre les cybermenaces avec le risque de charges excessives pour les entreprises. L'objectif n'est pas de compromettre la viabilité des entreprises avec des exigences irréalisables, mais de reconnaître que les cybermenaces préexistent à toute réglementation et

représentent un risque réel, comme en témoignent les attaques informatiques ayant entraîné parfois des faillites d'entreprises.

Agoria déploie plusieurs stratégies pour aider ses membres à naviguer dans ce cadre réglementaire complexe. Tout d'abord, l'organisation met un accent particulier sur la sensibilisation aux exigences du NIS 2. Pour ce faire, Agoria organise des campagnes d'information qui expliquent en détail les obligations découlant de cette directive et souligne l'importance de la conformité pour garantir la sécurité des réseaux et des systèmes d'information. Ces campagnes visent à assurer que les membres comprennent non seulement leurs responsabilités, mais aussi les implications de la non-conformité, notamment les risques pour la sécurité des infrastructures critiques. (De Kerchove, 2024)

Ils organisent de nombreuses conférences, notamment des sessions de 20 minutes, 40 minutes, voire 2 heures, pour leurs membres. Le but de ces conférences est de souligner l'importance de penser dès maintenant à la directive NIS2, même si leur travail sur ce sujet a débuté dès le début de 2023. Ainsi, ils fournissent une sensibilisation et une prise de conscience à leur communauté de membres. (Van Cangh, 2024)

En outre, Agoria ne se contente pas de sensibiliser ; l'organisation fournit également une assistance pratique pour aider les entreprises à se conformer aux exigences du NIS 2. Cela se manifeste par des offres telles que des sessions de formation spécifiques, des réponses aux questions individuelles et un large éventail de ressources en ligne. Ces services sont conçus pour guider les entreprises à travers les processus complexes de mise en conformité, en mettant l'accent sur les aspects pratiques et opérationnels de l'application des normes de sécurité prescrites.
Ce qu'ils font également, c'est d'identifier tous leurs membres qui opèrent dans le secteur manufacturier et qui présentent une maturité relativement faible en matière de cybersécurité. Ils élaborent ensuite un plan d'action, en visant spécifiquement à ce que 95% de leurs membres disposent d'un plan cyber. Certains membres qui ne sont pas directement concernés par la directive NIS2 sont encouragés à prendre en compte les questions de cybersécurité dans leur chaîne d'approvisionnement, afin de minimiser les risques. En revanche, pour ceux qui sont soumis à la NIS2, ils bénéficient de l'accompagnement du CCB (Centre Cybersecurity Belgium) ainsi que de la mise en place de ponts avec leurs partenaires, selon les pratiques actuelles.
Grâce à ces initiatives, Agoria s'affirme comme un pilier de support dans le paysage de la cybersécurité belge, en aidant les entreprises à naviguer dans les eaux souvent turbulentes de la conformité réglementaire tout en renforçant la sécurité globale de l'industrie technologique.

3.2.1.1 Académie NIS 2

Selon Arnaud Martin (2024), il devient nécessaire pour les entreprises de réfléchir à la méthodologie à suivre pour entamer ses démarches de mise en conformité, ainsi que les options d'implémentation de mesures de cybersécurité qui s'offrent à elles. Agoria répond à toutes ses questions en organisant l'Académie NIS2.

La volonté qui se cache derrière est qu'étant donné qu'il y a une organisation à mettre en place, que certaines mesures peuvent prendre du temps, et que d'autres demandent l'acquisition d'une certaine maturité, les entreprises ne doivent plus trop traîner pour entamer leurs démarches. Cependant, et cela a

pu être constaté lors des sessions d'informations sur NIS2, beaucoup d'entreprises manquent encore d'une direction claire, de démarches concrètes à suivre, à savoir par où et par quoi commencer.

Pour aider les entreprises à y voir clair et recevoir des conseils utiles sur la mise en conformité vis-à-vis de NIS2, l'Académie NIS2 a été lancée. Cette initiative a également été soutenue par des entreprises membres du business group Cyber Made in Belgium (CMiB) qui ont participé à des sessions de travail pour enrichir son contenu.

3 sessions ont déjà été mises en place et d'autres vont suivre. L'académie NIS2 se concentre sur l'orientation et le conseil pour la mise en œuvre des mesures NIS2. Elle clarifie les aspects théoriques et pratiques des obligations NIS2 au niveau belge (contexte, portée, impacts, mesures, options de conformité, supervision), et son objectif principal est de fournir un guide de démarrage rapide avec une méthodologie sur la façon de mettre en œuvre la directive étape par étape.

Cette académie s'adresse principalement aux personnes jouant un rôle dans la trajectoire de mise en œuvre de la conformité (informatique, sécurité, management) et qui fait partie soit des entités concernées par la directive NIS2, soit des fournisseurs des entreprises NIS2.

La formation est basée sur un point de vue légal, de bonnes pratiques à considérer et des recommandations pratiques d'experts en cybersécurité. Avec ce bagage l'entreprise ayant suivi l'académie pourra alors se diriger vers des consultants avec de meilleures connaissances.

3.2.2 NIS 2 catalyseur de la cybersécurité

Le NIS 2 se révèle être un catalyseur puissant pour la promotion de la cybersécurité, et Agoria est idéalement placée pour exploiter ce potentiel et soutenir ses membres dans cette démarche. En premier lieu, le NIS 2 a un impact significatif sur la sensibilisation des entreprises aux enjeux de la cybersécurité, en les incitant à reconnaître la sécurité des informations comme une priorité stratégique. Agoria tire parti de cette prise de conscience accrue pour encourager ses membres à investir davantage dans des mesures de sécurité robustes et adaptées. L'organisation joue un rôle d'éducateur et de guide, fournissant des ressources et des conseils pour aider les entreprises à comprendre et à implémenter les meilleures pratiques de sécurité. (Van Cangh, 2024).

Par ailleurs, le NIS 2 favorise une collaboration étroite entre les entreprises et les autorités compétentes afin d'assurer la résilience des réseaux et des systèmes d'information. Agoria facilite cette collaboration essentielle en organisant des événements, des forums et des initiatives de partage d'informations qui rassemblent des acteurs clés du secteur. Ces initiatives permettent non seulement un échange de connaissances et d'expériences, mais renforcent aussi le réseau de contacts entre les membres et les régulateurs, ce qui est crucial pour une réponse coordonnée aux incidents de cybersécurité.

En réalité, la partie juridique, qui concerne les obligations légales, revêt une importance cruciale lorsqu'il s'agit de modifier les mentalités ou d'améliorer une situation. Avec la digitalisation croissante des entreprises et l'augmentation des risques associés, notamment en termes de contrôles physiques liés aux outils informatiques, le besoin en cybersécurité est devenu indispensable.
Déclarer que la conformité à la NIS2 est une obligation légale pour certains acteurs les incitera à prendre cette question au sérieux lors de leurs discussions budgétaires. En effet, lorsqu'une entreprise évalue ses dépenses, elle accorde généralement la priorité aux obligations légales. Par exemple, si elle doit choisir

entre allouer des fonds à une mise en conformité NIS2 ou à un événement de team building, elle privilégiera généralement la conformité légale.
En fin de compte, il s'agit de se préparer à gérer efficacement un incident de cybersécurité ou même de l'éviter. La NIS2 n'est qu'un prétexte pour renforcer la cybersécurité, et de nombreux fournisseurs exploitent cette obligation pour promouvoir des solutions de cybersécurité supplémentaires.
De plus, dans ce contexte, il est important de rappeler à tous les acteurs concernés qu'ils sont tenus de respecter la loi. Les entreprises concernées doivent donc prendre des mesures spécifiques pour se mettre en conformité. Pour celles qui ne sont pas directement visées, il est crucial de considérer les risques encourus : une sécurité insuffisante peut entraîner le rejet par des clients importants cherchant à travailler avec des partenaires présentant moins de risques. (Vanden Geeten, 2024)

Ces entités impliquées contribueront à renforcer la résilience de l'ensemble de l'écosystème. Elles imposeront certaines exigences, et ceux qui s'y conformeront resteront dans le circuit. En revanche, ceux qui ne le feront pas prendront le risque d'être écartés.

Grâce à ces actions, Agoria se positionne comme un leader influent dans la promotion de la cybersécurité en Belgique, en utilisant le cadre du NIS 2 pour catalyser des changements significatifs et durables au sein de son réseau.

3.2.3 Outil de communication

De son côté, Agoria s'est fixé comme objectif que, d'ici 2025, 95% de ses membres auront un plan de cybersécurité. Dans le cadre de son engagement envers sa promotion, Agoria a mis en œuvre diverses initiatives et outils destinés à sensibiliser ses membres et à approfondir leur expertise dans ce secteur crucial. (Van Cangh, 2024).

J'ai eu l'opportunité de participer et de contribuer à la majorité des outils utilisés par Agoria. Cette expérience m'a permis de voir de l'intérieur comment ces outils fonctionnent, de discuter avec les entreprises membres et d'enrichir mon réseau professionnel.

Événements :

Les conférences, sessions plénières et événements spécialisés tels que le Forum International de la Cybersécurité (FIC), Europe CyberSec ou encore Milipol constituent des moments privilégiés que l'organisation saisit pour inviter l'ensemble des cadres exécutifs, ainsi que ses membres affiliés. À titre illustratif, lors de l'organisation du pavillon belge au FIC, Agoria a offert à ses membres une occasion inestimable d'échanger avec des délégués internationaux, facilitant ainsi la création de synergies et favorisant une intégration harmonieuse au sein d'un écosystème économique mondial. L'objectif d'Agoria est de garantir une intégration effective de ses membres, les empêchant de rester cloisonnés dans leurs sphères d'activité respectives. C'est la raison pour laquelle l'organisation met régulièrement en avant que l'adhésion à sa fédération représente bien plus qu'une simple cotisation ; elle constitue l'accès à un réseau privilégié, riche en informations spécialisées et en expertise partagée. En somme, adhérer à Agoria revient à intégrer un club exclusif où les membres bénéficient d'avantages distinctifs, garantissant ainsi leur satisfaction et leur engagement continu.

Cyberstart :

Cyberstart est l'un des projets phares par lesquels Agoria souhaite élever la conscience de ses membres quant à l'importance de la cybersécurité. Ce projet s'étend sur quarante semaines et comprend une série de quarante courriels, chacun fournissant des informations détaillées ainsi que des liens vers des vidéos incitant à l'action et à la sensibilisation. Initialement conçu en 2023 par Patrick Coomans pour la partie flamande de l'audience d'Agoria, ce programme a été adapté en français.

Eric Van Cangh est celui qui prête son nom et son image à cette version francophone affirme que « les retours sur cette initiative sont extrêmement positifs. Lors du Forum International de la Cybersécurité, on m'a même demandé si j'étais un robot ou une intelligence artificielle, preuve de l'impact marquant du projet. Je peux assurer que non seulement j'existe bel et bien, mais j'ai également participé activement à la révision de certains contenus, et je suis pleinement convaincu de la qualité des informations diffusées. Le contenu est de très haute qualité, et nos membres, ainsi que le public plus large, apprécie grandement cette ressource. » (Van Cangh, 2024).

Cyberstart est proposé gratuitement, tant aux membres qu'aux non-membres, dans le but de contribuer utilement à l'édification collective dans le domaine de la cybersécurité. Ce projet constitue une pièce essentielle du puzzle dans la lutte partagée contre les menaces cybernétiques.

On retrouve dans ces mails, les cinq grandes parties du NIST, à savoir Identify, Protect, Detect, Respond et Recover. Elles sont couvertes par une série de mails détaillant des actions spécifiques pour chaque domaine. Chaque domaine comprend environ une dizaine de mails, proposant des actions telles que la visualisation de vidéos, l'accès à des liens spécifiques, ou encore l'inscription au CCB, entre autres. Ces actions visent à faciliter l'intégration des membres dans un écosystème cybernétique, renforçant ainsi leur compétence dans différentes tâches. Après avoir suivi et accompli ces actions, les membres atteindront un certain niveau de maturité en matière de cybersécurité.

Formation de base : la cybersécurité en 30 étapes :

Cette formation est destinée pour toute personne désireuse de porter ses connaissances et sa compréhension de la cybersécurité à un niveau supérieur, la formation est payante. Elle offre une base excellente et complète, que l'on soit débutant dans le domaine ou que l'on cherche à actualiser ses connaissances. À l'issue de la formation, les participants sont bien informés sur les aspects essentiels de la cybersécurité, capable de mettre en œuvre des mesures de sécurité efficaces, et prêt à minimiser les risques de menaces numériques.

Digital Europe :

Agoria est également présente au sein de Digital Europe, la fédération européenne du numérique. Ils veillent à ce que les membres soient régulièrement informés des initiatives les plus significatives au niveau européen. Des experts Agoria s'engagent à recueillir les opinions des membres pour mieux défendre leurs intérêts auprès des institutions européennes via les canaux belges. Cette démarche s'inscrit dans le cadre des efforts de lobbying tant au niveau européen que belge.

Ils ont également pris en charge la préparation de l'initiative "En Route 2024" en vue des élections de juin. Ce projet vise à intégrer les priorités des membres d'Agoria dans les programmes des partis politiques pour les futurs gouvernements. Agoria a identifié entre dix et quinze thèmes prioritaires, incluant l'innovation, le talent numérique, l'environnement, l'énergie, etc. (De Kerchove, 2024).

3.2.4 CMIB

Le Cyber Made in Belgium (CMIB) est un regroupement business d'une centaine d'entreprises offrant des produits et des solutions cyber, initié par Agoria en 2021. Il fait partie de leur Digital Framework et représente le secteur économique de la cybersécurité aux côtés du CCB et de la Cyber Security Coalition, deux autres entités promouvant la cybersécurité. (Van Cangh, 2024).

La vision de ce projet est d'être la plateforme privilégiée donnant aux fournisseurs de services de cybersécurité en Belgique un visage, une voix et une écoute auprès de toutes les parties prenantes concernées (gouvernement, entreprises et citoyens en général). Leur mission est de supprimer les obstacles et de faciliter la création de catalyseurs pour l'adoption de la cyberrésilience en Belgique, soutenant ainsi la numérisation de la société dans son ensemble.

Différents objectifs sont poursuivis via ce comité, mais les principaux sont au niveau politique. L'idée est de sensibiliser les mondes politiques au fossé que la Belgique doit combler en matière de préparation à la cybersécurité. Cela implique d'être présent aux tables des gouvernements locaux, régionaux et fédéraux pour influencer la sensibilisation et les politiques visant à accroître la résilience cybernétique des entreprises, des gouvernements et des citoyens en général. Il s'agit également d'être à l'écoute des gouvernements sur la manière dont le secteur économique de la cybersécurité belge peut contribuer.

Au niveau sociétal, l'idée est de positionner la cybersécurité comme un catalyseur de la poursuite de la numérisation de la société dans son ensemble, tant pour les entreprises que pour la population en général. Au niveau économique, il s'agit de s'assurer de la création d'opportunités commerciales pour l'industrie cybernétique belge.

3.2.4.1 Les priorités

À la création de ce comité, la principale priorité était la réalisation d'une étude socio-économique afin de reconnaître l'industrie de la cybersécurité comme un secteur critique pour la société et l'économie belge, et de le faire savoir aux entreprises belges. Ce fut la première étude sur ce secteur. Pendant plus d'un an, des études qualitatives ainsi que des enquêtes quantitatives basées sur une base de données de 350 entités belges ont été menées. Agoria était soutenue par le ministère de la Défense et le Centre pour la Cybersécurité en Belgique, afin que chacun prenne conscience de l'énorme potentiel de la cybersécurité en Belgique.

Un autre objectif du CMiB est d'organiser des plénières. Ces plénières auxquelles j'ai pu participer, sont organisées par thème ou plus spécifiquement par groupe de focus du CMiB (CMiB4DEF, CMiB4TALENT et CMiB4ICS/OT) (figure 29). Elles ont généralement lieu en juin, septembre et décembre. En septembre, par exemple, CMiB4TALENT est au centre de l'attention lors de la plénière. Les réalisations et les lacunes sont discutées ainsi qu'un appel à l'action pour inciter de nouvelles personnes à rejoindre l'initiative, cela est complété par des intervenants invités qui viennent partager leurs expériences et leurs connaissances. Durant les CMiB4DEF des informations sensibles sont partagées, c'est le seul qui se tient en privé avec des personnes soigneusement sélectionnées et des personnes de très haut rang telles que des généraux ou des policiers.

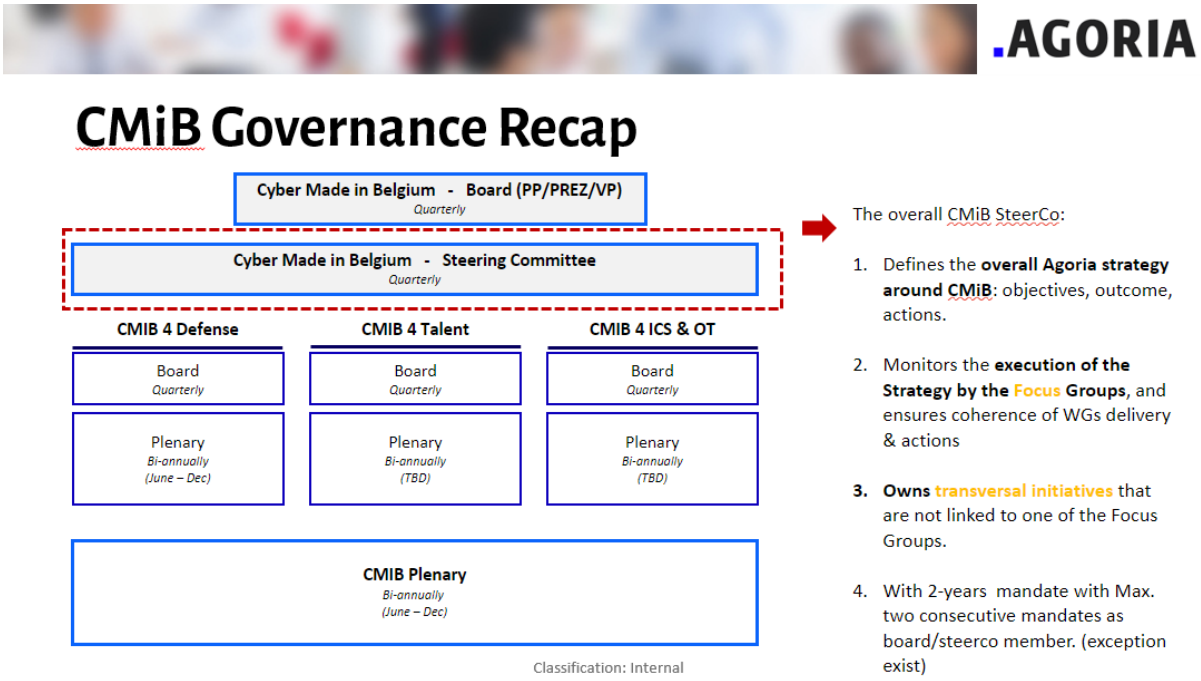


Figure 29: Composition et gouvernance CMiB
Agoria. (2022, novembre) *gouvernance CMiB* [Présentation Power Point]. Agoria

Le CMiB dans son ensemble a également son propre organe directeur, qui est le CMiB Steerco. Des acteurs importants de l'écosystème belge et des entreprises concurrentes se réunissent pour s'assurer que cette initiative reste sur la bonne voie. Ensemble, ils supervisent les activités des différents groupes de focus et travaillent sur leurs propres réalisations au sein du steerco. Quelques réalisations en 2023 incluent la création d'un roadshow appelée « Comment influencer le Leader » avec une vidéo enregistrée du Premier ministre Alexander de Croo, ou la participation au FIC (Forum International de la Cybersécurité) à Lille.

Le CMiB a de nombreux objectifs et réalisations à son actif, tous contribuant à l'écosystème de la cybersécurité en Belgique et visant à renforcer la résilience et la reconnaissance du monde complexe, mais incroyable que représente la cybersécurité. Comme expliqué précédemment, différents groupes de travail composent le CMiB, et c'est également la manière de fonctionner du Steerco. Cette année, quatre groupes de travail au sein du steerco cherchent à réaliser les priorités qu'ils ont définies.

Le premier groupe de travail, appelé **"Focus sur les élections de 2024",** souhaite créer un roadshow dédié aux élections qui auront lieu en Belgique. Leur objectif est de promouvoir l'agenda de la cybersécurité d'Agoria auprès des politiciens régionaux et fédéraux, afin d'influencer les priorités des futurs dirigeants. Ils espèrent réaliser cette tâche avec l'aide de 3 axes.
Le premier consiste à définir un ensemble de recommandations pour les différents niveaux politiques afin de les guider.
Le deuxième axe concerne l'organisation d'un événement avec des représentants de différents partis politiques, lors duquel l'objectif est de présenter les priorités d'Agoria et de permettre à ces représentants d'échanger avec des experts en cybersécurité.
Le troisième axe concerne la publication d'un document de position. Ce groupe de travail a également envoyé un sondage aux membres de l'écosystème afin d'obtenir leurs commentaires sur les politiciens, d'écouter les priorités qui doivent être abordées et de recueillir des recommandations.

Le deuxième groupe de travail, appelé **"Soutien/aide aux réalisations de CMiB4TALENT"**, visait à l'origine à aider les réalisations de CMiB4TALENT, l'un des propriétaires du groupe de travail faisant partie du conseil de CMiB4TALENT. Leurs objectifs auraient dû être de dresser la liste des exigences éducatives minimales pour la cybersécurité, d'analyser les besoins du marché et d'organiser des salons de l'emploi en cybersécurité. Cependant, il a été décidé d'alléger la tâche de ce groupe de travail, car elle faisait double emploi avec les tâches initiales de CMiB4TALENT. L'objectif maintenant est de voir ce qu'ils peuvent reprendre en charge et comment ils peuvent aider le parcours des talents.

Le troisième groupe de travail, appelé **"Tournée interne pour mettre en valeur les initiatives du CMiB"**, veut accroître la visibilité du CMiB à l'intérieur, mais aussi à l'extérieur d'Agoria. Pour augmenter leur visibilité externe, les membres de ce groupe de travail ont proposé diverses idées, allant de l'organisation d'un grand événement cyber en octobre 2024 à une éventuelle semaine de podcasts ou à l'investissement dans des bannières ou plus de publicité en général. Ils souhaitent occuper le terrain et créer différents discours dédiés à différents niveaux. Ils souhaitent également se concentrer sur l'aspect politique en organisant peut-être une table ronde avec des politiciens.

Enfin, le quatrième groupe de travail, **"Rencontre avec les investisseurs/clients - inviter les acteurs clés",** vise à créer des opportunités commerciales pour les membres du CMiB à la fois au sein de la communauté d'Agoria et avec les principaux acteurs économiques en Belgique. Ils souhaitent soutenir le développement économique de la communauté du CMiB en organisant des ateliers avec des experts et en invitant les principaux acteurs de la cybersécurité à rencontrer le marché.
Les objectifs vers lesquels ils travaillent sont ambitieux, mais aussi cruciaux pour atteindre leurs objectifs à long terme. Ces priorités sensibiliseront certainement les gens et les politiciens à l'importance de la cybersécurité et à la nécessité d'investir adéquatement dans ce domaine.

3.2.4.2 Les différents CMiB

Afin de réaliser ces priorités, le CMiB est divisé en trois groupes de réflexion : CMiB4DEF (défense), CMiB4TALENT (écoles et éducation) et CMiB4ICS/OT (industrie manufacturière). Ces groupes sont à nouveau subdivisés en différents groupes de travail qui ont tous des tâches et des objectifs différents. J'ai eu l'occasion de prendre part et m'impliquer dans ces différents groupes de travail et voir la façon dont cela fonctionne de l'intérieur.

CMiB Défense :

Le CMiB4DEF offre de multiples opportunités pour le développement de la résilience cybernétique au sein de la défense belge. L'objectif est de permettre aux membres de l'industrie d'aider la Force Civile de Résilience Cyber et de répartir les rôles et responsabilités en cas de crise majeure. Pour travailler sur cela, une équipe centrale du CMiB4DEF a travaillé sur la création de différents groupes de travail traitant de différents problèmes. Ces groupes de travail se sont tous réunis lors d'un atelier tenu en octobre et ont tous discuté individuellement de leurs objectifs, doutes et actions.

Le CMiB Défense vise à établir des synergies avec la Défense belge, dans le cadre du plan STAR (Sécurité/Service - Technologie - Ambition - Résilience). Ce plan, initié sous l'égide de la ministre de la Défense Ludivine Dedonder, définit les futures lignes politiques du département de la Défense. La

DIRS (Défense Industry and Research Strategy), quant à elle, promeut les synergies entre la Défense et les industries. Elle a défini 15 domaines de pointe auxquels un budget de plus de 1.8 milliard sera consacré jusqu'en 2030, avec la cybersécurité comme priorité absolue.

Grâce aux membres BSDI et CMiB, Agoria contribue à la mise en place de la 5e composante de la Défense, le Cyber Command. Ce dernier représente une avancée majeure dans la défense du pays contre les menaces cybernétiques.

Le premier groupe de travail porte sur : Feuille de route technologique pour le DIRS + Taxonomie. Sa mission est de fournir les contributions des membres du CMiB4DEF à la DIRS qui élabore une feuille de route technologique. Ils visent à fournir leurs contributions sur des sujets tels que les technologies clés, émergentes et perturbatrices ou les lacunes industrielles.

Le deuxième groupe de travail, intitulé Soutien au développement de la Force de Résilience Cyber, a pour objectif de motiver les principaux acteurs de l'industrie (entreprises ou individus) à faire partie de la Force de Résilience Cyber en cas de crise cybernétique.

Le troisième groupe de travail concerne "Le renforcement de la supply chain de la défense" en matière de cybersécurité. De nombreuses certifications différentes existent sur le marché et sont utilisées par différentes entreprises, l'objectif de ce groupe de travail est d'avoir une sorte de standardisation de ces certificats acceptée par différents organismes de réglementation comme le ministère de la Défense ou le gouvernement belge et les agences, et de comparer cela aux exigences de la défense.

Le quatrième groupe de travail vise à aborder le problème des "Compétences en cyberdéfense". Étant donné la sensibilité élevée du secteur de la défense, certains écarts existent entre les employés de l'industrie "normale" et ce que la défense requiert. Leur objectif est de créer une liste de ces écarts ainsi que de stimuler l'acquisition de compétences dans les domaines où des écarts sont présents. Ces compétences pourraient être acquises lors de CTF (Capture The Flag), par exemple.

Enfin, le cinquième groupe de travail concerne les "Salons, Événements et Communauté". Sa mission est de participer à des événements pertinents pour augmenter la visibilité du CMiB4Def. Cette visibilité pourrait être nationale, mais aussi internationale. Par conséquent, ils veulent créer une sorte de catalogue avec tous les événements et salons pertinents.

CMiB talent :

Le CMiB talent lui vise à répondre au problème existant des taux de poste vacant élevé en cybersécurité. En plus de cela, ils travaillent à combler les écarts entre les compétences acquises à l'école et celles demandées sur le marché du travail.
Selon l'étude menée par Agoria dans le secteur de la cybersécurité, on parle de plus de 1200 postes vacants et de ± 4000 dans tous les secteurs combinés. Tout comme le groupe de focus précédemment mentionné, le groupe de focus CMiB4TALENT est divisé en différents groupes de travail, traitant de sujets différents et travaillant sur différents plans d'action. (Van Cangh, 2023)

Le premier groupe de focus, appelé "Mapping and Forecasting", travaille sur trois sujets principaux. Tout d'abord, ils veulent cartographier les offres de formation et d'éducation en cybersécurité. Cela ne se limite pas seulement aux universités et à l'enseignement supérieur, mais aussi aux formations non régulières ou publiques. Un exemple en est Molengeek, dont la mission est de rendre le secteur

technologique accessible aux personnes n'ayant pas de parcours traditionnels ou ne disposant pas du niveau d'éducation considéré comme approprié.

Le groupe de travail suivant se concentre sur "l'amélioration de l'expertise en cybersécurité dans les entreprises", car cela n'est pas toujours acquis. Pour y parvenir, leur plan d'action se concentre sur quatre sujets principaux. Le premier, concerne les employés et vise à créer une Académie CMiB qui a pour objectif de créer des formations pour les employés selon certains parcours de carrière. Ensuite, ils veulent travailler sur le reclassement en établissant des partenariats avec le VDAB/FOREM ou d'autres centres de compétences et acteurs clés de la cybersécurité pour créer des formations pour les personnes qui ont décidé de changer de parcours professionnel et d'entrer dans le domaine de la cybersécurité. Leur troisième plan d'action est de créer un atelier sur le recrutement qui serait coordonné par l'Académie Agoria. Enfin, ils veulent trouver des partenaires pour organiser un salon de l'emploi CyberTalents avec des universités et d'autres partenaires d'Agoria pour attirer de nouvelles personnes et des jeunes dans le domaine.

L'objectif du troisième groupe de travail est de créer "Plus d'afflux dans les études et formations en numérique/cybersécurité". Pour y parvenir, ils veulent promouvoir le numérique et la cybersécurité dans différents niveaux d'éducation, organiser des actions de sensibilisation à la cybersécurité pour les jeunes en collaboration avec des partenaires, organiser des visites d'écoles avec des entreprises de confiance pour parler de cybersécurité et organiser des témoignages.

Enfin, le quatrième groupe de travail, appelé "Travailler avec les Universités/Écoles Supérieures & Centres de Formation", travaillera sur trois sujets principaux. Mettre en place un groupe d'experts sur divers sujets de sécurité dans les universités. Ils veulent organiser une académie d'été pour "former les formateurs" et donner aux enseignants la possibilité de rencontrer des experts et de réseauter. Enfin, ils veulent développer le concept d'alternance, comme en France, qui est une sorte d'apprentissage en milieu de travail tout en étudiant à l'école.

CMiB Manufacturing :

Ce focus group est le plus récent, j'ai eu la possibilité de participer à sa création. Il s'agit ici du secteur manufacturier avec ICS, qui signifie Industrial Control Systems, et OT, qui signifie Operational Technology, ce sont des composants essentiels des infrastructures critiques telles que les centrales électriques, les réseaux d'eau, les usines de fabrication, et d'autres installations industrielles. ICS/OT est un terme qui englobe les systèmes de contrôle industriel et les technologies qui supervisent et contrôlent les processus physiques.
Les enjeux de la cybersécurité liés aux ICS/OT sont particulièrement élevés, car ces systèmes sont souvent critiqués pour la sécurité nationale et le bien-être économique. Les entreprises manufacturières sont clairement vulnérables face aux attaques informatiques parce qu'elles travaillent avec du matériel de production souvent obsolète (« legacy systems ») et pourtant de plus en plus connecté. Trop souvent dans l'industrie, l'IT est considéré comme un coût, donc une contrainte. Aujourd'hui la question n'est plus « SI je vais être attaqué », mais « QUAND vais-je être attaqué ? ».

Ce groupe de focus a été créé pour aider et offrir une campagne de sensibilisation aux deux tiers des membres d'Agoria appartenant à ce secteur. Lors de la première réunion d'introduction, l'objectif d'Agoria, représenté par Eric Van Cangh et Alain Wayenberg, était d'expliquer la finalité du CMiB et de déterminer les groupes de travail qui semblaient les plus judicieux pour chacun des membres. De

cette réunion a été décidée la création de six groupes de travail. Leur contenu n'a pas encore été déterminé, mais de prochaines réunions sont prévues afin de décider qui seront les différents leaders pour chaque groupe de travail, ainsi que les tâches et missions respectives. Les différents groupes de travail sont : la sensibilisation du Top management, des évènements et salons sur l'OT, les infrastructures critiques en OT, le partage de connaissances et talent en OT, accompagnement des PME. D'ailleurs la directive NIS 2 a élargi sa portée, de nombreux secteurs manufacturiers seront désormais concernés, d'où la création de ce focus group CMiB4ICS/OT.

Au final l'objectif ici est de mettre la cybersécurité à l'agenda de toutes les entreprises membres d'Agoria. La volonté est de faire passer le message qu'investir dans la cybersécurité ne représente pas un coût, mais une valeur ajoutée, qui se traduit par deux mots-clés : trust & resilience. Créer de la confiance, notamment dans le chef des clients, et assurer la continuité du business en cas d'incident. Les deux sont intimement liés, car montrer que l'on est capable de continuer à travailler et tenir debout, malgré un désastre – qu'il soit physique ou cyber d'ailleurs – va augmenter la confiance du monde extérieur. Cette résilience est un véritable état d'esprit à adopter au quotidien pour chaque entreprise, un mode de travail.

3.3 Conclusion intermédiaire

Ce chapitre m'a permis de découvrir en profondeur les efforts déployés par Agoria pour promouvoir la cybersécurité en Belgique, ainsi que les différentes initiatives visant à sensibiliser, former et accompagner les entreprises dans leur démarche de sécurité informatique. L'analyse a mis en lumière plusieurs problématiques majeures auxquelles l'écosystème belge est confronté.

Premièrement, le nombre élevé de postes vacants en cybersécurité a conduit au lancement d'initiatives telles que CMiB4TALENT, visant à attirer et former des professionnels dans ce domaine. Malgré ces efforts, le manque de talent en cybersécurité demeure un défi majeur pour les entreprises, rendant difficile le renforcement de leur résilience face aux cybermenaces.

Deuxièmement, la faible maturité en cybersécurité du secteur manufacturier est préoccupante. Beaucoup d'entreprises de ce secteur utilisent des systèmes obsolètes qui augmentent leur vulnérabilité aux cyberattaques. La création du focus group CMiB4ICS/OT vise à remédier à cette situation en sensibilisant et en accompagnant ces entreprises vers une meilleure préparation.

Troisièmement, il existe un besoin critique d'harmonisation et de standardisation des certifications en cybersécurité, ce qui est particulièrement pertinent pour les secteurs sensibles comme la défense. Le manque de standards clairs et reconnus complique la tâche des entreprises qui cherchent à se conformer aux exigences de sécurité.

La directive NIS 2 sert de catalyseur puissant pour la promotion de la cybersécurité. En imposant des obligations légales claires et en renforçant les exigences de sécurité, elle incite les entreprises à investir dans des mesures de cybersécurité robustes. Cette directive met en lumière l'importance de la cybersécurité comme priorité stratégique, non seulement pour la conformité légale, mais aussi pour la protection des infrastructures critiques et la continuité des opérations.

L'importance de la cybersécurité ne peut être sous-estimée. Elle est essentielle pour protéger les données sensibles, assurer la confiance des clients, et maintenir la résilience opérationnelle face aux cybermenaces de plus en plus sophistiquées. La cybersécurité est encore vu comme un coût pour les entreprises et non comme un bénéfice ou un avantage.

En transition vers le prochain chapitre, j’explorerai une analyse empirique avec des propositions concrètes sur la manière d'effectuer un changement efficace dans une entité concernée. J’examinerai comment les entreprises peuvent intégrer les exigences de la directive NIS 2 dans leurs pratiques et devenir véritablement "cyber résilientes".

Section 4 : Analyse empirique

4.1 Introduction

À l'approche de la mise en application de la directive NIS 2, prévue pour le 18 octobre 2024, il devient impératif pour les entités régulées d'adopter une approche proactive face à ces nouvelles exigences réglementaires. La plupart des entreprises n'ont pas encore atteint l'étape de conformité, soulignant l'importance d'anticiper et de proposer des actions concrètes pour aider les entités concernées à se préparer efficacement.

Après avoir exploré la littérature sur le sujet et présenté un plan d'action pour promouvoir l'adhésion des entreprises à la directive et à la cybersécurité, il est temps d'analyser les entretiens et de proposer une feuille de route pour la mise en place de cette directive.

Cette section du mémoire se propose d'examiner en profondeur l'impact potentiel de la directive sur les organisations concernées. Mon objectif est double : réaliser un état des lieux initial de l'impact de ce changement réglementaire et, sur cette base, développer un ensemble structuré de stratégies et d'actions concrètes. Ces actions sont conçues pour non seulement faciliter la transition vers la conformité, mais aussi maximiser les bénéfices organisationnels à long terme de cette adaptation.

4.2 Le changement

« Le changement est devenu le maître mot des projets organisationnels. La capacité de changer, pour une organisation, n'est plus une compétence ponctuelle pouvant être achetée à l'extérieur, mais un actif immatériel à construire, consolider et développer.» (Autissier et al, 2018)

La mise en œuvre de la directive NIS 2 dans une entreprise peut être perçue comme un changement important ou complexe selon la définition donnée, car elle implique une rupture significative des modes de fonctionnement habituels pour se conformer à de nouvelles normes de cybersécurité. Cette transition vers un futur conforme à la NIS 2 est synonyme de progrès, notamment en termes de sécurité des informations et des réseaux.

4.3 L'alignement stratégique

Selon Henderson et Venkatraman (1993), une stratégie d'alignement est essentielle pour assurer la cohérence et l'harmonie entre les différents aspects d'une organisation.
En tenant compte des exigences de la Directive NIS 2, qui stipulent dans son article 20 que l'organe de direction des entités approuve les mesures de gestion du risque de cybersécurité prises par ces entités afin de se conformer à l'article 21, en supervisent la mise en œuvre et peuvent être tenus pour responsables des violations.

Les organes de direction doivent donc s'assurer entre autres que la structure de gouvernance, les politiques de cybersécurité, l'établissement des objectifs de sécurité, sont alignés sur l'appétit de l'entité pour le risque et compatible avec l'orientation stratégique de l'organisation.

La perspective d'alignement « Strategy Execution» du modèle de Venkatraman paraît la plus pertinente et judicieuse pour l'implémentation au sein d'une entreprise. (Figure 30)

Voici comment cette perspective peut être appliquée à l'implémentation de la Directive NIS 2 :

- **Business Strategy** : Définir la réponse stratégique de l'entreprise aux exigences de la NIS 2, en alignement avec les objectifs commerciaux globaux et les obligations de conformité. Cela comprend l'établissement d'objectifs et de politiques clairs de cybersécurité dictée par la direction.
- **Organizational Infrastructure :** Développer ou ajuster les structures organisationnelles pour soutenir la stratégie de cybersécurité. Cela pourrait inclure l'établissement d'un cadre de gouvernance de la cybersécurité, la nomination de rôles tels que le Responsable de la sécurité des systèmes d'information (RSSI), et la création d'équipes interdépartementales pour gérer les risques de cybersécurité.
- **IT Infrastructure** : Aligner l'infrastructure IT pour supporter l'exécution de la stratégie de cybersécurité. Mettre en place les technologies et systèmes nécessaires pour la gestion des risques de cybersécurité, le reporting des incidents, et assurer que les aspects technologiques de l'organisation soutiennent l'opération sécurisée et la résilience de l'entreprise.

Adopter cette perspective garantit que la cybersécurité n'est pas confinée en tant que question technique, mais est intégrée à chaque couche de l'entreprise, depuis la prise de décision jusqu'aux opérations quotidiennes. En effet, il est essentiel de comprendre que la cybersécurité ne devrait pas être considérée uniquement comme une question technique gérée par le département informatique, mais plutôt comme une préoccupation qui affecte l'ensemble de l'entreprise. La directive exige que les entreprises identifient, évaluent et atténuent les risques liés à leurs systèmes d'information critiques. Cela ne concerne pas seulement les risques techniques, mais également les risques opérationnels, financiers et de réputation.
Les équipes de direction doivent donc travailler en collaboration avec les équipes de sécurité informatique pour élaborer des stratégies de gestion des risques efficaces.

Le but est de créer une culture de la sécurité solide est essentielle pour garantir que chaque employé comprend et prend au sérieux les enjeux de la cybersécurité. Cela va au-delà de la simple sensibilisation à la sécurité informatique et implique de promouvoir des comportements sécurisés dans tous les aspects du travail. Les formations en sécurité, les politiques de sécurité claires et la responsabilisation des employés sont des éléments clés pour développer cette culture.

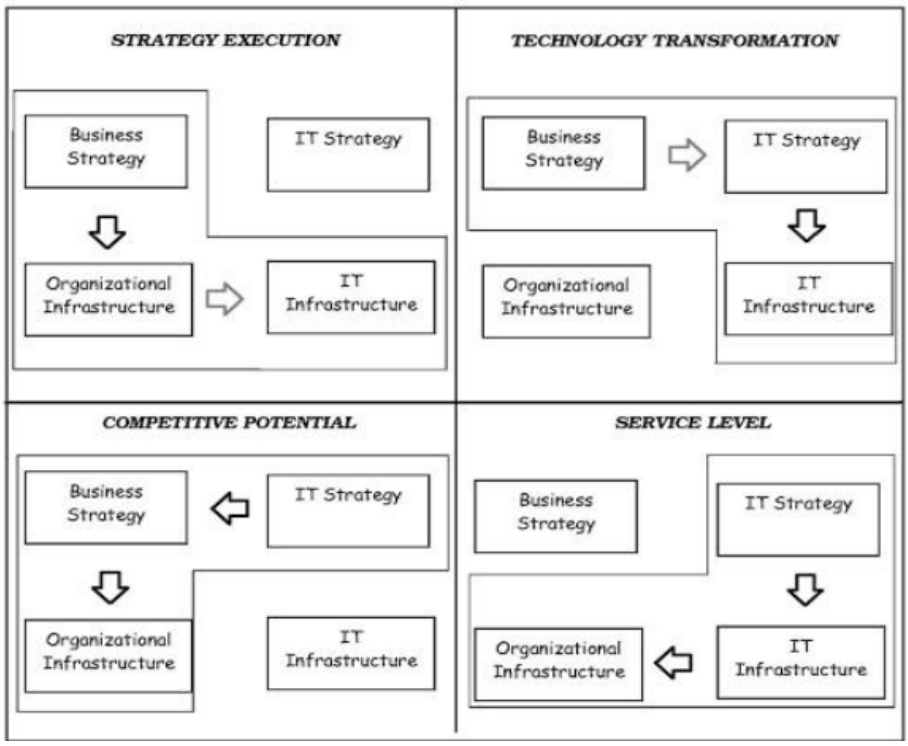


Figure 30: Perspective d'alignement

Source : Henderson, J.C., & Venkatraman, N. (1993). *Strategic alignment: Leveraging information technology for transforming organizations*. IBM Systems Journal, 32(1), 4-16.

4.4 Comprendre le changement

4.4.1 Typologie du changement

Mais de quel type de changement s'agit-il ?

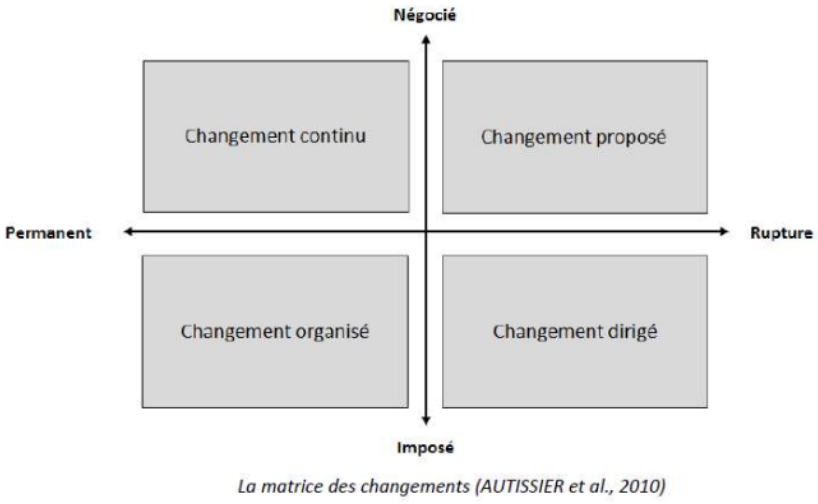


Figure 31: Typologie du changement

Source : Autissier, D., Moutot, J. M., & Charbonnier, O. (2010). *Le changement organisationnel : Théories et Pratiques.* Dunod

Le changement dirigé (figure 31) correspond à la mise en œuvre de la directive NIS 2, car ce type de changement est caractérisé par son aspect obligatoire et son origine externe à l'organisation. Il est déterminé par une autorité ou un régulateur, en l'occurrence l'Union européenne, ce qui fait de lui un changement qui n'est pas optionnel et qui doit être suivi. Les entités doivent se conformer aux exigences réglementaires spécifiques, ce qui requiert pour certaines d'entre elles une refonte des politiques de sécurité, des processus, et peut-être même de l'infrastructure IT. Ce changement n'est pas négociable et doit être exécuté dans des délais impartis, ce qui nécessite une planification et une direction claire de la part de la direction pour assurer une transition en douceur vers les nouveaux standards requis.

Comprendre le type de changement, tel que le changement dirigé pour la directive NIS 2, est crucial, car cela définit la manière dont l'organisation doit aborder ce changement. Il informe la direction sur la nécessité de suivre un plan structuré et détaillé, imposé par des exigences réglementaires externes. Cela influence directement les stratégies de gestion du changement, la mobilisation des ressources, la communication interne, et l'élaboration des plans de formation. En d'autres termes, la reconnaissance du type de changement oriente l'ensemble du processus de transition vers les nouveaux standards de cybersécurité, garantissant ainsi une mise en conformité réussie et durable.

En mettant en pratique ce modèle, nous avons une meilleure perception du changement, ce qui permettra de proposer des stratégies adéquates pour gérer cette transition. L'objectif est d'augmenter les chances de réussite du changement tout en minimisant les résistances. En mobilisant les employés et en créant un environnement propice à l'adaptation et à l'innovation, car un des autres enjeux majeurs pour le top management est de promouvoir et fournir une formation à leur collaborateur, ainsi qu'à eux même.

4.4.2 Lieu du changement

La directive NIS 2 implique une transformation profonde au sein des organisations, touchant à plusieurs aspects clés de leur fonctionnement. Le changement est une rupture et elle nécessite donc une révision des pratiques existantes, notamment en matière de sécurité informatique, en introduisant de nouvelles procédures et normes de sécurité. De plus, elle exige des changements au niveau des conditions de travail, avec une amélioration des infrastructures informatiques pour assurer une protection adéquate des données sensibles. Les outils informatiques et de gestion doivent également être repensés pour répondre aux exigences de sécurité élevées imposées par la directive. Sur le plan organisationnel, la directive NIS 2 exige une réorganisation des responsabilités et des processus décisionnels, avec la désignation de responsables de la sécurité et la création de comités dédiés à la cybersécurité. Les entreprises doivent également investir dans le développement des compétences et des savoir-faire de leur personnel pour s'adapter aux nouvelles exigences. La stratégie globale de l'entreprise doit être alignée sur les objectifs de sécurité de la directive, intégrant la cybersécurité comme une priorité stratégique. Enfin, la culture organisationnelle doit évoluer pour promouvoir une mentalité axée sur la sécurité, sensibiliser les employés à l'importance de la cybersécurité et renforcer les valeurs liées à la protection des données. En adoptant cette approche holistique, les organisations peuvent mieux se préparer aux défis de la cybersécurité et garantir une protection efficace de leurs systèmes d'information critiques. (Autissier et Moutot, 2010)

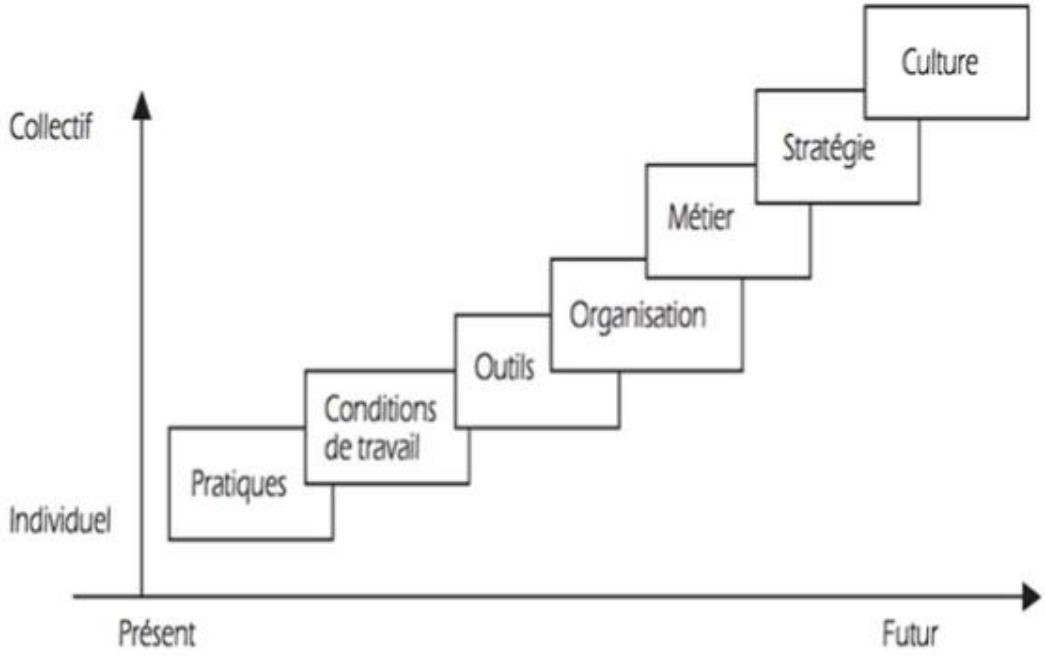


Figure 32: Les lieux du changement
Source : Autissier, D., Moutot, J. M., & Charbonnier, O. (2010). *Le changement organisationnel : Théories et Pratiques.* Dunod

Le processus de changement induit chez les personnes qui doivent le vivre une série de pertes, allant bien au-delà des simples modifications de pratiques ou de procédures. Ces pertes comprennent, entre autres, la perte de certitudes quant à la stabilité de leur environnement de travail, la perte de prévisibilité concernant leur rôle et leurs responsabilités, ainsi que la perte de pouvoir sur les décisions qui les affectent directement.

Les pertes prennent une dimension particulière dans le contexte de la cybersécurité. Avec la menace constante de cyberattaques potentielles. La perte de prévisibilité liée à la nature évolutive des menaces cybernétiques, qui peut changer rapidement et de manière imprévisible. La perte de pouvoir ressentie par les individus qui doivent se conformer à de nouvelles règles et réglementations en matière de sécurité, souvent sans pouvoir influencer ces décisions.

4.5 Diagnostique de la directive

Le diagnostic d'un changement est une évaluation systématique qui vise à comprendre l'état actuel d'une organisation afin de préparer efficacement la mise en œuvre de nouvelles initiatives ou politiques. Cette démarche analytique permet d'identifier les besoins de changement, les forces sur lesquelles s'appuyer et les obstacles à surmonter. L'objectif principal est de créer une feuille de route claire qui guide l'organisation à travers le processus de changement en minimisant les risques et en maximisant les chances de succès.

Dans le contexte de la directive NIS 2, le diagnostic de changement est particulièrement pertinent. La NIS 2, étant une réglementation visant à renforcer la sécurité des réseaux et des systèmes d'information au sein de l'UE, impose aux organisations concernées de nombreux ajustements tant au niveau technologique qu'organisationnel.

L'utilité du diagnostic de changement se manifeste au niveau stratégique où il offre une vision claire de la direction à prendre pour atteindre la conformité, alignant les initiatives de changement avec les objectifs stratégiques de l'entreprise. Au niveau opérationnel il permet de mettre en œuvre des changements de manière ordonnée et systématique, en s'assurant que chaque étape contribue efficacement à la conformité globale. Finalement au niveau culturel il prépare le terrain pour une culture de sécurité renforcée, essentielle pour la réussite à long terme des objectifs de la directive NIS 2.

Cependant, chaque entreprise aura des spécificités en fonction du secteur où elle se trouve, de sa taille, ou encore de son organigramme. Par conséquent, il faudrait adapter cette étude et cette qualification en fonction de sa propre entreprise. Ici, je vais réaliser un diagnostic de qualification et quantification sur le cadre général de la directive qui concerne tout le monde et voir l'impact qu'il aura sur les entités concernées. Pour obtenir quelque chose de plus précis à son secteur ou à son entreprise, il faudrait adapter ce cadre à son entreprise en prenant en compte des axes plus pertinents et spécifiques. Il serait également nécessaire de refaire des interviews pour mener cette conduite du changement.

4.5.1 Qualification du changement

Pour diagnostiquer efficacement un changement, l'utilisation d'un outil de qualification du changement se révèle particulièrement utile. Cet outil, structuré sous forme de tableau, comprend une série de questions qui évaluent divers aspects du projet et de son contexte. Ces questions couvrent les méthodes, les outils à déployer, les ressources nécessaires, et d'autres facteurs pertinents qui influencent la gestion du changement.

L'intérêt de cet outil réside dans sa capacité à produire un diagnostic préliminaire du changement dès les premières étapes de planification. En posant des questions stratégiques dès le début, l'outil amène les gestionnaires de projet à réfléchir sur la manière dont ils vont conduire le changement, et à anticiper les défis potentiels. Chaque question est associée à un score qui aide à évaluer la complexité inhérente à chaque aspect du changement. En sommant ces scores, il est possible de juger globalement si le changement est simple, important, ou complexe.

L'utilité de cet outil se manifeste notamment par sa capacité à permettre un audit express du projet de changement. Cette évaluation rapide aide à visualiser la complexité du changement, facilitant ainsi la prise de décision sur les approches et les ressources nécessaires pour mener à bien le projet. En conséquence, cet outil est non seulement un facilitateur de planification, mais aussi un moyen efficace d'aligner les stratégies de gestion de changement avec les exigences réelles du projet, garantissant ainsi une meilleure adaptation et mise en œuvre de la directive NIS 2 au sein de l'organisation.

J’ai donc créé un tableau Excel avec de nombreuses questions sur la conduite du changement lors de l’implémentation de la directive. Des questions avec pour axes : la culture, l’emploi, l’organisation, le management, la performance, les processus et le légal. Sur base de ses questions, j’ai proposé des réponses que j’ai pondérées en fonction de l’impact qu’ils auront sur la mise en place d’une conformité

à la directive. L'objectif étant de voir les points qui poserait problème ainsi que la complexité de ce changement au sein des entités concernées.
J'ai posé donc mes différentes questions à des experts en cybersécurité et NIS 2 qui savent quels sont les enjeux que les entités feront face lors de l'implémentation des mesures de la directive.

Ces experts sont Valery Vander Geeten, responsable juridique du centre de la cybersécurité en Belgique (Annexe 6 : Interview Valery Vanden Geeten), Eric Van Cangh cybersécurité business group leader au sein d'Agoria (Annexe 8 : Interview Eric Van Cangh), ainsi que Pieter Batsleer et Antoine Debuisson consultant en cybersécurité chez Nviso. (Annexe 10 : Interview Nviso)

Pour mener à bien ces entretiens, j'ai créé un guide avec des questions regroupées selon leurs caractéristiques, qui sont elles-mêmes regroupées selon des concepts plus globaux. Ces entretiens étaient de type semi-dirigé, c'est-à-dire que j'avais ma liste de questions que je posais, et mon interlocuteur avait la liberté de répondre à la question et d'aborder d'autres thématiques selon son ressenti. Les questions étaient donc ouvertes et les sujets abordés étaient variés.

Pour ce qui est du CCB et Agoria, ils ont créé des groupes de travail pendant plus d'un an, où ils ont vu à la fois les administrations publiques, les secteurs publics et les administrations privés, entre autres, BELTUK, la Cyber Security Coalition, la FEB et ils ont fait des brainstormings, des discussions, des premiers jets, etc. Afin de discuter sur comment appliquer cette directive ce que les entités sont obligés de faire. Les outils qu'ils peuvent mettre à disposition, en tenant compte des avis des concernés. Ils ont fait aussi toute une consultation publique sur le projet de loi et l'arrêté royal pour justement avoir l'input d'un maximum de personnes, d'identités.

Bien sûr, en définitive, c'est le niveau politique qui décide, c'est le parlement qui décide, c'est l'Organisme qui décide. Mais ces entités doivent être conseillés, c'est pourquoi Agoria accompagné du CCB doivent leur amener une proposition, car il faut venir avec une proposition concrète et c'est ce qu'ils ont fait en tenant compte au maximum des intérêts ou des conseils, des commentaires des uns des autres.

Les entreprises sont conscientes du risque de cybersécurité, elles comprennent pourquoi il leur est demandé d'augmenter leurs exigences par rapport à ça. Mais il y'a une crainte par rapport à ce que représentent les contrôles, de l'impact pour leur business, de leur compétitivité de manière générale. Donc le comité qui se regroupe tient en compte de ça aussi parce que l'objectif ce n'est pas de couler les entreprises sur base d'exigences qui sont démesurées ou disproportionnées.

Pour ce qui est de Nviso, j'ai eu la possibilité d'avoir le côté client et entités concerné et les insights de consultants qui travaillent sur la mise en place de la conformité à la directive. Actuellement NIS 2 est un très grand sujet pour eux, une grande préoccupation pour beaucoup de leurs clients. Ils les aident principalement à évaluer les lacunes et l'état de préparation, à élaborer des feuilles de route et à les aider dans la mise en œuvre.
Leurs clients leur posent beaucoup de questions à ce sujet. Il peut s'agir de comprendre, par exemple, s'ils sont dans le champ d'application, s'ils sont concernés, s'ils ont besoin d'aide.

Choix des axes :

Culture :

La culture organisationnelle est essentielle pour la réussite de toute initiative de changement. Dans le contexte de la directive NIS 2, une culture de sécurité forte est cruciale. Les entreprises doivent sensibiliser leur personnel à l'importance de la cybersécurité et les impliquer activement dans les efforts de conformité. Une culture de sécurité bien établie favorise la conformité volontaire aux politiques et procédures de sécurité, réduisant ainsi les risques de violations et de non-conformité. De plus, les formations et les accès aux différentes données des entreprises dépendent des employés, ce qui nécessite leur implication à tous les niveaux et une conscience cyber. C'est pourquoi développer une culture se trouve être un axe clé. Il s'avère que ce sera un réel chalenge, car ces aspects culturels ne peuvent pas être changés du jour au lendemain et qu'il faudra du temps, plusieurs mois voire plusieurs années.

Emploi :

Les changements induits par la directive NIS 2 peuvent avoir un impact sur l'emploi au sein de l'organisation, mais du secteur de la cybersécurité en général. Par exemple, il peut être nécessaire de recruter des experts en cybersécurité supplémentaires, de former le personnel existant ou même de revoir certains postes pour inclure des responsabilités liées à la sécurité de l'information. Une gestion efficace des aspects liés à l'emploi garantit que les ressources humaines sont adaptées aux besoins de conformité et que le personnel est motivé et compétent pour soutenir les efforts de sécurité.

Organisation :

La structure organisationnelle doit être alignée sur les objectifs de conformité de la directive NIS 2. Cela peut impliquer des ajustements dans les rôles et les responsabilités, ainsi que dans les processus de communication et de prise de décision. Une organisation bien structurée facilite la mise en œuvre efficace des mesures de sécurité et garantit une coordination appropriée entre les différents départements et équipes impliqués.

Management :

Le leadership joue un rôle crucial dans la conduite du changement. Les cadres supérieurs doivent montrer l'exemple en soutenant activement les initiatives de conformité et en fournissant les ressources nécessaires. De plus, ils doivent être capables de communiquer clairement les objectifs de sécurité et de motiver le personnel à les atteindre. Un management fort favorise l'engagement des employés et facilite l'adoption des nouvelles pratiques de sécurité.

Performance :

La performance organisationnelle est directement liée à la conformité à la directive NIS 2. Des mécanismes de mesure efficace permettent d'évaluer régulièrement les progrès réalisés et d'identifier les domaines nécessitant une amélioration. Cela peut inclure des indicateurs de performance clé (KPI) liés à la sécurité des systèmes d'information, tels que le nombre de failles détectées, le temps de réaction aux incidents, etc. Une gestion proactive de la performance garantit une conformité continue et une résilience face aux menaces. De plus, les entreprises concernées sont loin de la maturité qu'ils devraient atteindre. En particulier, si on regarde le cadre Cyber Fundamentals, on y trouve les niveaux de maturité qu'il faut atteindre en tant qu'entreprise importante et essentielle. Si l'on s'en tient strictement à ce cadre et qu'on applique à tous ces contrôles, un grand nombre d'entreprises, voire la quasi-totalité d'entre elles, n'obtiendront pas de bons résultats, car leur maturité est assez faible.

Processus :

Les processus organisationnels doivent être adaptés pour intégrer les exigences de la directive NIS 2. Cela implique la création de nouveaux processus ou la mise à jour de ceux existants pour garantir une gestion efficace des risques liés à la sécurité de l'information. Les processus de surveillance, de gestion

des incidents, de gestion des changements et de sensibilisation doivent être spécifiquement examinés et ajustés. Des processus bien définis et cohérents facilitent la mise en œuvre des mesures de sécurité et garantissent une conformité soutenue.

Juridique :
La conformité à la directive NIS 2 implique également une compréhension approfondie et une application rigoureuse des aspects juridiques liés à la cybersécurité. La garantie que les contrats avec les fournisseurs et partenaires respectent les standards de sécurité exigés, et la mise en œuvre de procédures légales pour la réponse aux incidents et la gestion des violations de données.

Les réponses que j'ai obtenues via les différentes interviews m'ont permis de compléter le tableau. Pour chaque réponse, j'ai attribué un poids en fonction de l'impact plus ou moins important qu'elle aura sur chaque axe. (Annexe 2). Les réponses quant à elle sont disponibles dans les différentes retranscriptions des interviews.

Exemple de question :

Les entités sont-elles prêtes à faire face à ce changement ?
Axe : performance
Proposition : oui, non, mitigé
Poids : 0, 4, 2

Réponse de Valery :

Cela ne se fera pas du jour au lendemain. Sinon, les entreprises ne savent pas être prêtes. Même si, en théorie, avec déjà le RGPD, et certains avec déjà le NIS 1, etc., elles devraient déjà être conformes ou elles devraient déjà être prêtes.
Mais quand même, il y a encore un gap, il y a quand même des efforts à faire. Donc, on a fait en sorte qu'on cède aux entités 18 mois et puis 12 mois. Pour qu'elles passent d'abord du niveau de base, qu'elles soient au niveau basic, et après elles passent au niveau important, et après encore au niveau essentiel.

Réponse d'Éric :

Le milieu manufacturier, par exemple, a une maturité relativement assez pauvre. Et on met un plan d'action, justement, le 25% de nos membres ont un plan cyber. (priorité d'Agoria auprès de ses membres) Certains membres qui ne sont pas vraiment dans le NIS2, on va les inciter à la supply chain, faire attention, essayer d'avoir des impacts. Et ceux qui sont dans le NIS2, les accompagner avec les outils du CCB et de faire les bridges avec tous nos partenaires comme on fait maintenant. Les entreprises dont les grosses ont déjà la majorité des mesures qui sont respectées et donc ils auront une liste et devront juste coche que tout est OK, alors que pour les PME leur maturité est encore très faible.
On fait une journée spéciale en Wallonie, en français, pour le milieu manufacturier des petites PME. C'est une journée intense, une journée complète, où d'abord j'ai l'honneur de pouvoir faire l'ouverture, le keynote, sur justement l'écosystème, les menaces, etc. Pour les sensibiliser sur pourquoi investir. Et puis on a d'autres collègues qui vont investir sur la partie plutôt théorique, les outils disponibles, les

aspects financiers que la région offre, etc. Comme ça ils ont toutes les armes en main, ils sont au courant, ils ont les outils, ils ont les contacts. Voilà, c'est tout ce qu'on fait.

Analyse :

Valery souligne qu'il existe un délai de mise en conformité, avec des étapes progressives (niveau de base, important, essentiel) sur une période de 18 mois puis 12 mois.
Il mentionne que malgré l'existence de réglementations antérieures comme le RGPD et le NIS 1, de nombreux efforts restent à faire.
Ce commentaire indique que même si les entreprises devraient déjà être prêtes en théorie, il existe un écart (gap) significatif entre les exigences actuelles et le niveau de préparation réel des entreprises.

Eric souligne une faible maturité dans le milieu manufacturier en matière de cybersécurité.
Il mentionne qu'une proportion importante de PME n'ont pas encore adopté de mesures de sécurité adéquates et que leur maturité est encore très faible.
Pour combler ce manque de préparation, des actions de sensibilisation et de formation sont mises en place par Agoria, notamment avec des journées intensives dédiées à la cybersécurité.

Les commentaires de Valery et d'Eric mettent en lumière le fait que l'implémentation de la directive NIS 2 nécessite un travail continu et des efforts soutenus, indiquant ainsi une réponse mitigée quant à la préparation actuelle des entreprises à faire face à ce changement.

Cette analyse des deux réponses me pousse à choisir la proposition mitigé et donc d'accorder une pondération de 2 à cette question et donc pour l'axe performance.

Pour voir le reste des questions, elles se trouvent à l'annexe 2 quant aux réponses elles se trouvent dans la retranscription des différentes interviews faites avec les experts.

4.5.2 Quantification du changement

Ensuite, sur base de ce tableau avec les différentes questions, il faut procéder à une étude de l'impact des cadrans qui constitue une méthode quantitative.

L'objectif principal de cette méthode est de générer un résultat quantitatif, souvent sous forme de graphique radar, qui illustre clairement les domaines les plus exposés aux changements induits par la directive. Ce graphique radar permet de visualiser l'ampleur de l'impact dans différents secteurs ou aspects de l'entreprise, offrant ainsi une vue d'ensemble de la portée des adaptations nécessaires.

L'utilisation d'un cadran pour mesurer les impacts est une caractéristique clé de cette approche. Le cadran n'est pas seulement un outil de mesure, mais aussi un moyen de structurer l'analyse en catégorisant les différents types d'impacts, qu'ils soient stratégiques, opérationnels, technologiques ou humains. Cela aide les décideurs à comprendre les multiples facettes du changement et à prioriser les interventions.

Il est important de noter que, bien que cette méthode fournisse une mesure quantitative des lieux de changements, elle ne définit pas le contenu spécifique de ces changements. Autrement dit, elle identifie où les efforts doivent être concentrés, mais ne spécifie pas les actions précises à entreprendre. C'est pourquoi l'étude de l'impact des cadrans est souvent suivie d'une analyse qualitative plus détaillée qui explore comment les changements devraient être mis en œuvre.

Enfin, l'établissement d'un graphique radar suite à l'analyse permet de présenter visuellement les résultats de l'étude. Ce graphique est particulièrement utile lors des réunions avec les parties prenantes, car il fournit une représentation immédiatement compréhensible de l'impact du changement, facilitant ainsi les discussions stratégiques et aidant à aligner les équipes sur les priorités du projet.

Cette méthode d'étude de l'impact des cadrans, en combinant des analyses quantitatives et qualitatives, offre aux responsables de projet un outil efficace pour naviguer dans les complexités de la mise en œuvre de la directive NIS 2, assurant ainsi une transition plus réussie et moins risquée pour l'organisation.

En utilisant la méthode des cadrans, inspirée du modèle d'Autissier, j'ai généré un graphique radar qui illustrera quantitativement les domaines les plus affectés par la mise en œuvre de cette directive.

L'objectif de cette étape quantitative est de fournir une visualisation claire de l'impact dans différentes sphères comme les opérations, la technologie, les ressources humaines, et la stratégie. Le cadran, en tant qu'outil central de cette méthode, nous aidera non seulement à identifier les zones d'impact, mais aussi à hiérarchiser les actions à entreprendre en fonction de leur urgence et de leur importance. Ce processus implique une évaluation systématique des réponses recueillies lors des entretiens avec des experts, transformant des données qualitatives en un ensemble de mesures quantitatives qui seront ensuite représentées sur le graphique radar.

Graphique radar généré	
Organisation	4,33333333
Culture	4,25
Management	4,5
Processus	4,33333333
Emploi	4,5
Performance	3,33333333
Legal	2,33333333

Figure 33: Pondération du graphique radar

Ce premier tableau, présente les scores moyens obtenus pour chaque aspect évalué sur une échelle de 1 à 5, où 5 indique que le changement aura un gros impact dessus et 1 l'impact du changement est assez faible.

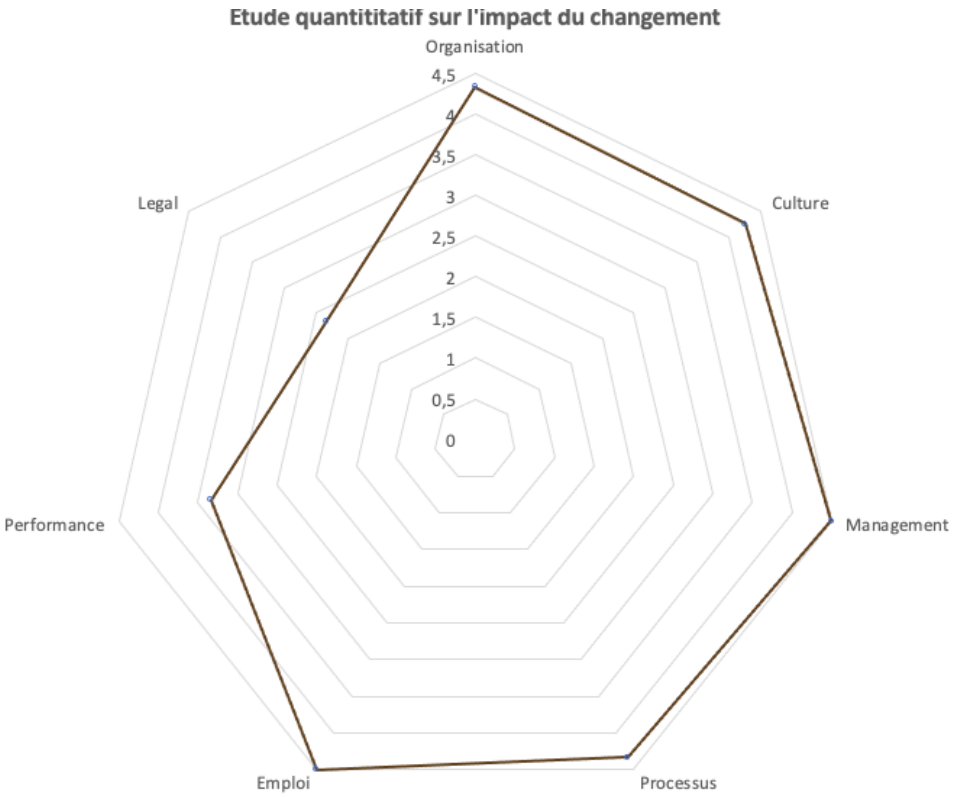


Figure 34: Graphique Radar

Ce qui me génère un graphique comme celui-ci présenté ci-dessus. Les axes du radar montrent clairement que l'organisation, la culture, le management, les processus, et l'emploi seront très impactés par la mise en place d'une conformité à la directive NIS 2. Cependant, les domaines de performance et surtout légal subiront un impact moins accru, comme illustré par leurs scores relativement plus bas.

Sur une échelle de 100, j'obtiens un score supérieur à 70, ce qui signifie que **le changement est considéré comme complexe**. Il est complexe, car il touche tous les aspects de l'entreprise que ce soit la gouvernance et le top management que l'employé de bureau. On parle ici, comme détaillé tout au long du mémoire, d'une directive européenne qui vise à augmenter la cyberrésilience des entités qui ont un aspect critique dans la société et l'économie. Pour cela certains changements drastiques doivent être menés.

De plus, la cybersécurité est vue comme un coût par les entreprises. Donc c'est toujours une bataille pour les managers en cybersécurité et les CISO d'obtenir un budget et avec l'obligation d'implémentation d'une si grosse directive, il faut énormément de budgets parce que soit on embauche, soit on prend des consultants, mais il faut abattre la charge de travail à un moment ou à un autre. Il y'a également les certifications, les licences pour certains programmes, etc. Ce sont tous des coûts qui s'accumulent et le management n'y voit pas l'intérêt, ce qui rajoute une couche de complexité au problème.

Tout l’enjeu se tourne alors sur cette nécessité de sensibiliser et promouvoir la cybersécurité et cette directive auprès des tops manager. Les informer, communiquer, accompagner, ce sont toutes des étapes essentielles à la bonne réalisation des exigences demandées.

Dans l'Annexe 3, vous trouverez un ensemble de mesures tirées des cadres référentiels ITIL et COBIT pour faciliter le processus de changement. Ces cadres fournissent des lignes directrices et des meilleures pratiques pour la gestion des services informatiques et la gouvernance des technologies de l'information. En intégrant ces référentiels, l'annexe propose des outils et des stratégies pour améliorer l'efficacité, la sécurité, et la conformité des systèmes informatiques pendant les périodes de transition. Ces mesures sont essentielles pour garantir un changement structuré et contrôlé au sein des organisations.

4.6 Communiquer le changement

Sans un plan de communication et un pilotage efficace, des craintes et des préoccupations peuvent émerger au sein des entités concernées, ce qui pourrait mettre en péril la mise en place des nouvelles mesures. Le but est d’accompagner l’ensemble de ses collaborateurs dans ce processus qui demandera certains gros changements pour les entités.

Les craintes et préoccupations peuvent être néfastes pour la mise en place d'un changement pour plusieurs raisons. Tout d'abord, elles peuvent engendrer une résistance au changement parmi les employés, les incitant à s'opposer activement ou passivement aux nouvelles mesures. Cette résistance peut ralentir ou même bloquer la mise en œuvre réussie du changement. De plus, les craintes et les préoccupations non adressées peuvent générer de l'anxiété, du stress et de l'insatisfaction parmi les employés, ce qui peut entraîner une diminution de la motivation et de la productivité. En outre, elles peuvent entraîner une perte de confiance dans la direction et le processus de changement, ce qui compromet l'engagement des employés envers les objectifs du changement. Enfin, si les craintes et les préoccupations ne sont pas prises au sérieux et ne font pas l'objet d'une communication transparente, elles peuvent se propager rapidement dans toute l'organisation, créant un climat de méfiance et de scepticisme qui nuit à la cohésion et à la collaboration. En résumé, il est essentiel de reconnaître et d'adresser les craintes et préoccupations des employés de manière proactive afin de favoriser une transition réussie vers les nouvelles mesures. (Autissier et al., 2018)

4.6.1 Les outils de communication

Ce tableau (figure 35) présente une classification des outils de médias utilisés dans un plan de communication, organisée en trois catégories : médias froids, communication permanente, et rencontres. Chaque catégorie joue un rôle crucial dans la structuration et l'exécution efficace d'un plan de communication, en particulier dans des contextes de changement organisationnel, comme l'implémentation de la directive.

Médias froids		Médias chauds
Communication institutionnelle	**Communication permanente**	**Rencontres**
Kit de communication Plaquette, dépliant Affiches Mails animés Kit de lancement	Journal interne Documentation Site web Articles Journal interne Vidéos	Réunion d'information Réunion questions/réponses Réunion de pilotage du projet Rendez-vous individuels Comités Groupes de travail

Tableau. Outils Média (Autissier et Al, 2019)

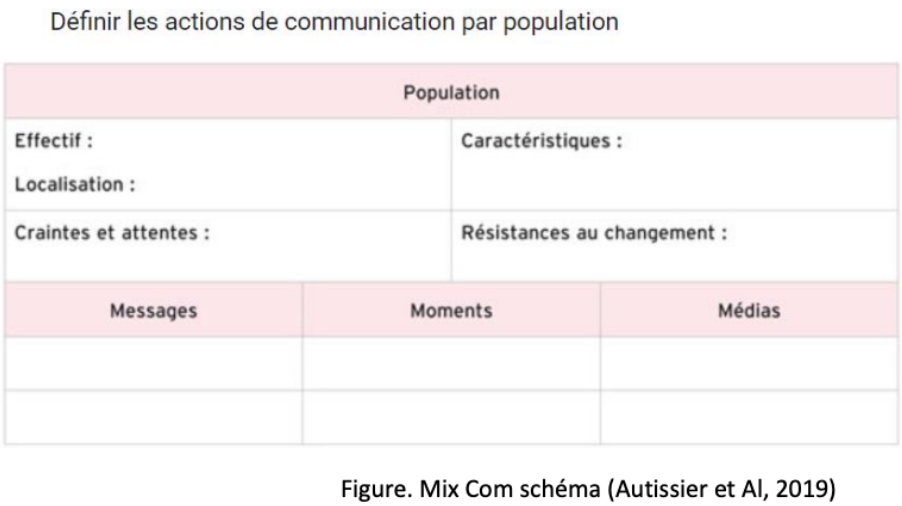
Figure 35: Supports pour transmettre les arguments du projet

Autissier, D., & Al. (2019). *Outil 36. Le plan de communication.* cairn.info. https://www.cairn.info/la-boite-a-outils-de-la-conduite-du-changement--9782100776344-page-108.htm

L'utilisation combinée de ces différents outils médiatiques dans un plan de communication aide à assurer que tous les niveaux de l'organisation sont correctement informés, engagés et capables de contribuer à la mise en œuvre effective du changement. Ces outils aident à créer une stratégie de communication complète qui peut répondre à divers besoins et styles d'apprentissage, maximisant ainsi les chances de succès du projet de changement.

4.6.2 Mix Com

Le "Mix Com" est une fiche stratégique qui permet de définir et de formaliser les actions de communication pour des groupes cibles spécifiques au sein d'une organisation. Cet outil est particulièrement utile lors de la mise en œuvre de grands changements, où il est crucial de communiquer efficacement pour gérer les perceptions, attentes et résistances.


Définir les actions de communication par population

Population	
Effectif : Localisation :	Caractéristiques :
Craintes et attentes :	Résistances au changement :

Messages	Moments	Médias

Figure. Mix Com schéma (Autissier et Al, 2019)

Figure 36: Mix com

Autissier, D., & Al. (2019). Outil 36. *Le plan de communication.* cairn.info. https://www.cairn.info/la-boite-a-outils-de-la-conduite-du-changement--9782100776344-page-108.htm

Il est indispensable dans la gestion de changement, permettant de créer une stratégie de communication personnalisée et efficace. Par son approche structurée, il assure que tous les aspects de la communication sont couverts et alignés avec les besoins spécifiques des bénéficiaires du changement. Cela est particulièrement crucial dans des projets d'envergure tels que l'implémentation de la directive NIS 2, où la réussite dépend en grande partie de la capacité à gérer les perceptions et à engager positivement toutes les parties prenantes dans le processus de changement.

4.6.3 Plan de communication

Finalement le plan de communication est un document ou une feuille de route qui décrit les objectifs de communication, identifie les publics cibles, définit les messages clés à communiquer, et établit les canaux et les calendriers pour la diffusion de ces messages. L'objectif principal d'un plan de communication est de fournir des informations pertinentes et nécessaires aux parties prenantes de manière organisée et stratégique, pour influencer les perceptions, encourager l'adoption de changements, ou promouvoir des comportements spécifiques.

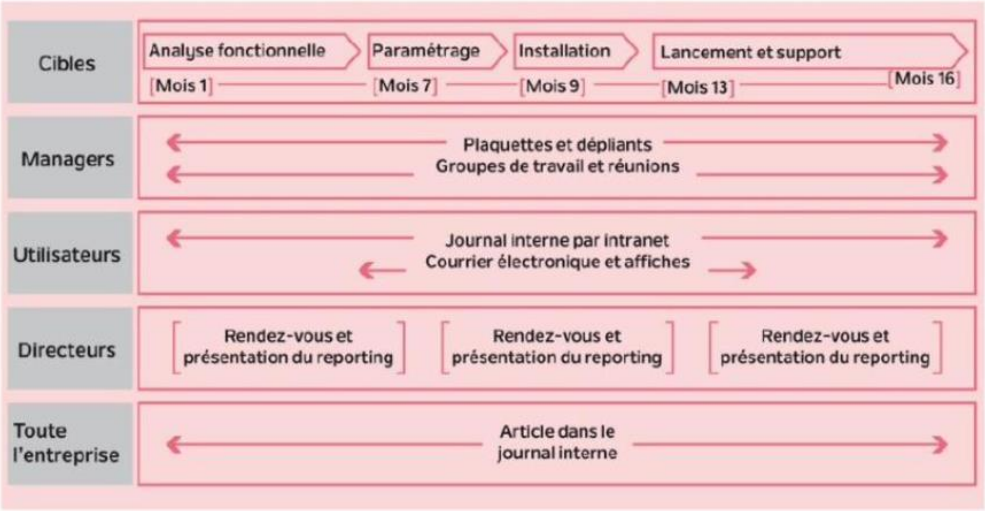


Figure. Plan de communication(Autissier et Al, 2019)

Figure 37: Plan de communication

Autissier, D., & Al. (2019). Outil 36. *Le plan de communication.* cairn.info. https://www.cairn.info/la-boite-a-outils-de-la-conduite-du-changement--9782100776344-page-108.htm

Au sein même des entités concernées, l'établissement d'un plan de communication joue donc un rôle crucial dans la réussite de la mise en conformité. Celui-ci va articuler comment les stratégies de communication seront déployées à travers les différentes phases d'un projet de changement. Il sert de guide pour aligner les messages, les cibles, les moments et les médias, garantissant ainsi que la communication est cohérente, opportune et efficace à chaque étape du processus.
Il constitue un outil de prévision des actions de communication en fonction des cibles et des phases du projet de changement. Le plan de communication est l'outil clé du levier de communication et prend en général la forme d'un panorama. Le plan de communication transforme les messages définis dans le mix communication en actions, dans un plan global. Il sert de calendrier des échéances, de base pour les hypothèses budgétaires et de moyen de coordination avec les autres actions du projet. (Autissier & Al, 2019)

Au niveau d'Agoria, la communication est également un pilier essentiel pour diffuser toutes les informations essentielles sur la mise en place de la directive NIS 2, ce qu'elle représente et ses implications. La conscientisation est une étape critique dans ce processus, car elle vise à sensibiliser et à informer les membres d'Agoria sur les enjeux de la cybersécurité et sur les exigences spécifiques de la directive NIS 2.

Agoria a utilisé une stratégie de communication claire et cohérente pour informer ses membres sur la directive NIS 2. Cela passe par l'organisation de sessions d'information, de webinaires ou de séminaires sur la cybersécurité et la directive NIS 2, animés par des experts en la matière. Ces événements permettent aux membres d'Agoria de comprendre les implications spécifiques de la directive pour leur secteur d'activité et les mesures qu'ils doivent prendre pour se conformer. (cf. supra p.82) Agoria se sert également des tribunes qu'elle possède lors d'événements, qu'elle organise ou auxquels elle participe, pour parler de cela. (cf. supra p.84)

4.7 Co-construire le changement

Dans le cadre de l'implémentation de la directive NIS 2 au sein des entités, il est essentiel d'adopter une approche de co-construction collaborative, en intégrant directement les employés et autres parties prenantes impactées par les changements réglementaires. Comme le montre le chapitre précédent sur l'importance de la communication dans les processus de changement, l'annonce de nouvelles directives peut susciter des craintes et des préoccupations parmi le personnel. Selon Autissier (2019), afin d'atténuer ces craintes-là, il est primordial d'impliquer les bénéficiaires du changement afin de les faire vivre dans le processus de transition, et en adoptant une telle méthode, cela les encouragerait à participer au changement. Cette participation favorise l'acceptation et l'engagement envers le changement. Comme expliqué le bouleversement dans les entités concernées est réelle et la préparation

Pour faciliter la co-construction du changement au sein d'une entreprise, il est essentiel de mettre en place des structures et des méthodologies qui organisent et dynamisent l'engagement des parties prenantes. Parmi ces méthodologies, le modèle RACI, l'atelier Speed Boat et participatif se distinguent comme des outils particulièrement efficaces pour structurer la participation et clarifier les rôles et responsabilités au sein du projet de changement.

4.7.1 Matrice RACI

L'acronyme anglo-saxon RACI est une méthode pour définir les niveaux de responsabilité d'activités au quotidien ou dans le cadre d'un projet, notamment de changement.
Pour chaque activité sont définis :

- **R (Responsible)** : responsable de production, s'assure de la réalisation d'une activité de ou de la production d'un livrable.
- **A (Accountable)** : La personne qui est ultimement responsable et a le dernier mot sur l'achèvement de la tâche.
- **C (Consulted)** : Les personnes qui doivent être consultées avant une décision ou une action, généralement celles qui ont une expertise ou des informations nécessaires.
- **I (Informed)** : Les personnes qui doivent être informées de la décision ou de l'action, généralement celles qui sont affectées par l'issue, mais n'ont pas de rôle actif dans son élaboration.

L'utilisation du modèle RACI dans le cadre de la mise en œuvre de la directive NIS 2 aide à clarifier qui est responsable de quelles actions au sein du projet, réduisant ainsi les confusions et les chevauchements de responsabilités. Cela assure également que toutes les parties prenantes sont adéquatement consultées et informées, favorisant une communication fluide et une prise de décision efficace. (Autissier & Al, 2019)

4.7.2 Atelier Speed Boat et participatifs

L'atelier Speed Boat est une technique de rétroaction agile qui permet aux équipes de réfléchir aux obstacles et aux accélérateurs de leur projet. Dans cet atelier, l'équipe est invitée à imaginer leur projet comme un bateau tentant d'atteindre un objectif. Les obstacles qui ralentissent le bateau (le projet) sont

identifiés comme des ancres, tandis que les éléments qui pourraient le faire avancer plus rapidement sont vus comme des moteurs.

Il s'utilise soit en démarrage de projet pour partager une vision et anticiper sa mise en œuvre, soit en cours ou fin de projet pour un bilan ou une rétrospective.
L'atelier peut consister en un petit groupe composé de l'équipe responsable de l'implémentation de la directive sur un atelier participatif. L'équipe pourra se fixer différents objectifs, faire un état des lieux des mesures déjà en place et celles qui nécessiteront un investissement que ce soit pécuniaire ou de temps. Voir également quels types de résistances ils font ou feront face lors de l'implémentation.

Il serait aussi opportun d'organiser des ateliers participatifs (figure 38), qui correspondent au modèle de co-construction du changement développé par Autissier. Ces ateliers ont pour but d'échanger et de résoudre des problèmes tout en favorisant la collaboration. (Autissier et al., 2019) Celui-ci commencerait par une séance de "Catharsis". Les employés auront l'occasion de partager leurs craintes et leurs ressentis concernant le changement. Prévoir de consacrer des séances de questions/réponses pour répondre aux interrogations des employés. S'en suivra un atelier de Brainstorming pour pouvoir apporter des suggestions et propositions. Après, un atelier d'exploration pour pouvoir communiquer sur la mise en œuvre. Et enfin, cela se terminera par un atelier de décisions à laquelle le comité de décision de l'entreprise pourra y être associé. (Autissier et al., 2019)

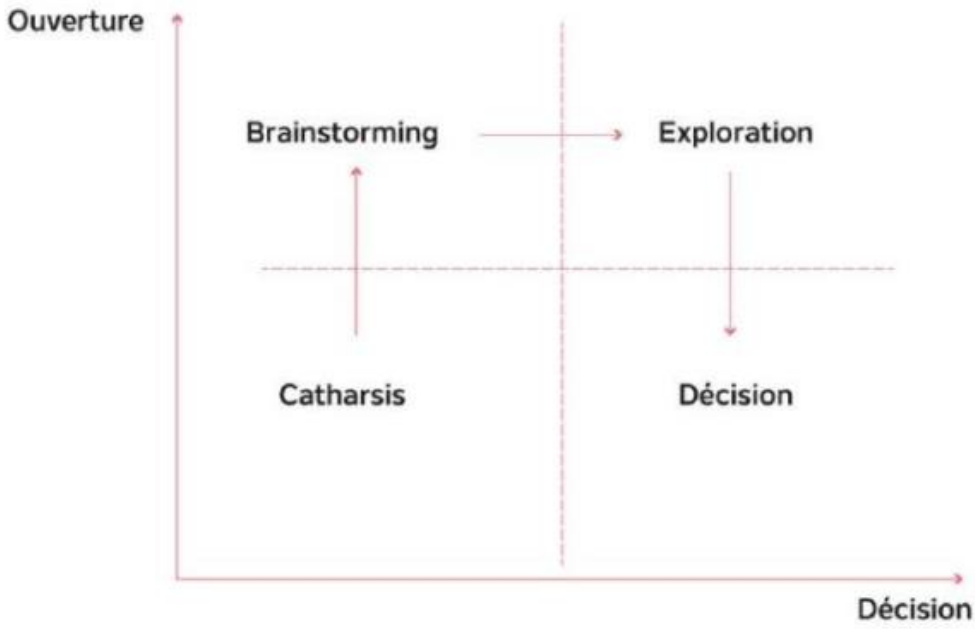


Figure 38: La matrice des ateliers participatifs
Autissier, D., & Al. (2019). Outil 36. *Le plan de communication.* cairn.info. https://www.cairn.info/la-boite-a-outils-de-la-conduite-du-changement--9782100776344-page-108.htm

4.8 Accompagner et piloter le changement

L'accompagnement du changement est une étape cruciale afin de permettre aux entités d'effectuer ce changement de manière efficace et de s'adapter facilement à cette nouvelle manière de travailler et de s'organiser. L'accompagnement facilite ce processus en réduisant les résistances et en favorisant l'engagement des parties prenantes.

L'implémentation de la directive NIS 2 est susceptible d'entraîner des changements profonds et étendus au sein des entités concernées, affectant non seulement les aspects technologiques, mais également la culture, la structure organisationnelle et les processus. Ces transformations nécessitent une gestion délicate et proactive pour garantir une transition fluide et efficace.

Pour accompagner ces changements, il est impératif de mettre en place une équipe spécialement dédiée au changement. Cette équipe aura la responsabilité de soutenir les employés et de gérer les diverses initiatives nécessaires à une adaptation réussie. Les actions envisagées incluent l'organisation de workshops destinés à introduire et à intégrer la nouvelle culture d'entreprise, ainsi que des sessions d'information pour familiariser le personnel avec les nouvelles régulations et procédures.

Prévoir des sessions de team building pour renforcer la cohésion et la collaboration internes, éléments clés pour naviguer avec succès à travers les périodes de changement.
Mettre un point d'honneur sur la bonne communication et collaboration avec des discussions entre les employés, des discussions entre les différents départements. C'est un point qui revient beaucoup, mais il est essentiel pour la bonne mise en place d'un changement et accompagner ses parties prenantes.

Ces initiatives sont conçues pour non seulement faciliter l'adoption des nouvelles pratiques et technologies, mais aussi pour renforcer l'engagement et l'adhésion des employés au nouveau système. En prenant ces mesures, les entités pourront mieux gérer l'impact organisationnel et culturel de la directive NIS 2, minimisant les perturbations tout en maximisant l'efficacité de leur mise en conformité.

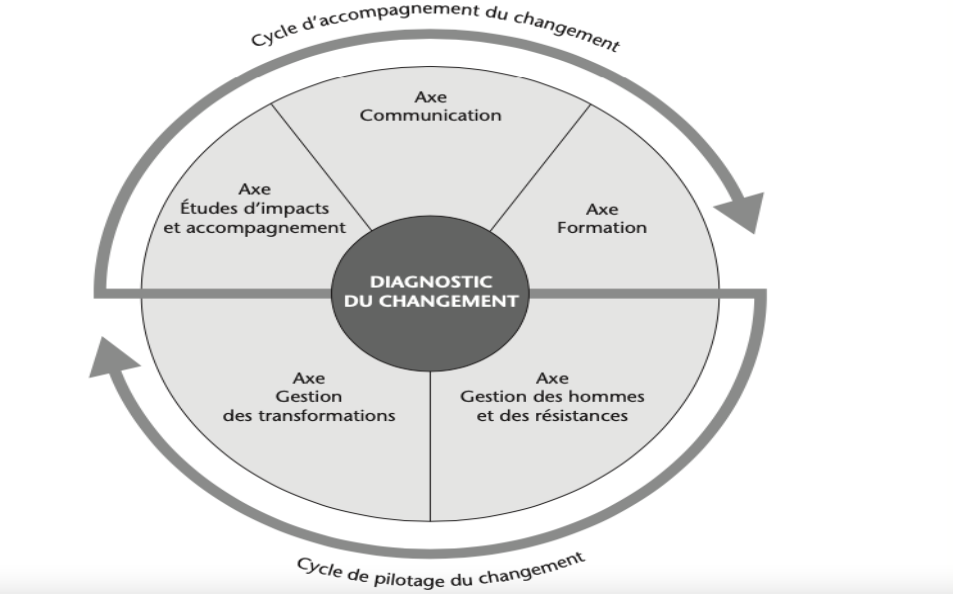


Figure 39: Méthode de conduite du changement
Autissier, D., Vandangeon-Derumez, I., Vas, A., & Johnson, K. P. (2018). *Conduite du changement : Concepts clés.* Dunod.

4.8.1 Plan de Pilotage

Le plan de pilotage détaille les étapes clés et les actions nécessaires pour la mise en œuvre des mesures de conformité avec la directive NIS 2 (Network and Information Systems Security) au sein des entreprises. Ce plan est conçu pour guider les entreprises à travers un processus structuré afin d'assurer la sécurité et la résilience de leurs réseaux et systèmes d'information.

Le projet concerne n'importe quelles entités concernées par la directive, le but ici est de donnée une feuille de route sur comment piloter ce changement. Des différences se feront d'une entité à l'autre en fonction de son niveau de maturité, son niveau de cybersécurité, son budget, etc. Avec une aptitude au changement évaluée comme faible pour la plupart des entreprises et un budget évalué approximativement à la hausse d'environ 700k€. Ce chiffre provient d'une discussion avec des consultants de chez Nviso, qui ont calculé le nombre de Man-days pour le projet ainsi que le salaire nécessaire. On se retrouve avec cette fourchette à la hausse. (Batsleer & Debuisson, 2024)
La stratégie de changement est co-construite, impliquant une équipe de deux experts en conformité et cybersécurité, ce nombre peut augmenter ou diminuer en fonction de l'entreprise. En général la durée pour réaliser l'évaluation complète est de 3 ans c'est-à-dire 36 mois.

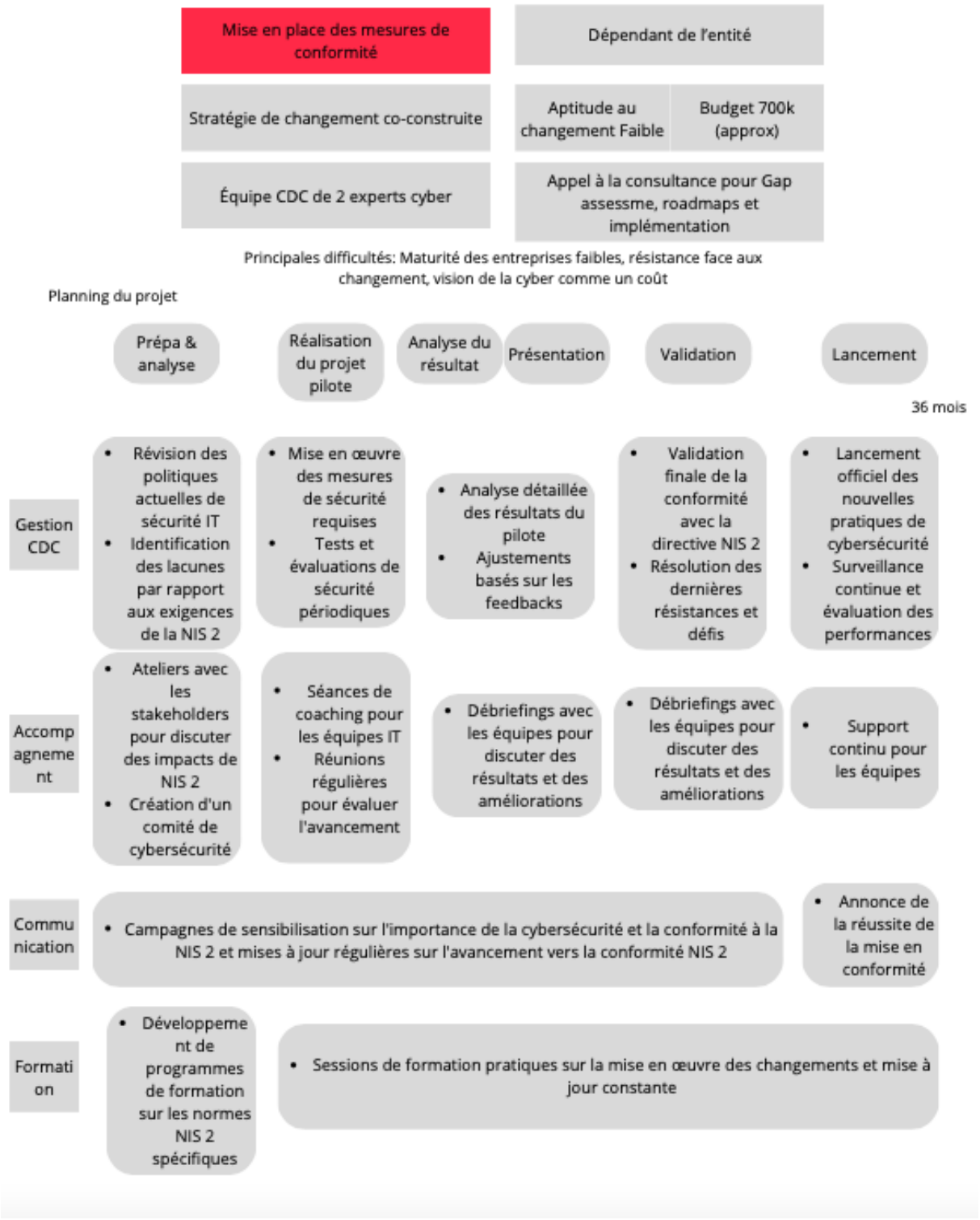


Figure 40 : Plan de pilotage

Phases du Projet

1. **Préparation et Analyse**
    - **Gestion CDC** (comité du changement): Révision des politiques actuelles de sécurité IT et identification des lacunes par rapport aux exigences de la directive NIS 2.
    - **Accompagnement** : Organisation d'ateliers avec les parties prenantes pour discuter des impacts de NIS 2 et création d'un comité de cybersécurité.

- **Communication** : Lancement de campagnes de sensibilisation sur l'importance de la cybersécurité et la conformité NIS 2.
- **Formation** : Développement de programmes de formation spécifiques aux normes NIS 2.

2. **Réalisation du Projet Pilote**
   - **Gestion CDC** : Mise en œuvre des mesures de sécurité requises et réalisation de tests et évaluations périodiques.
   - **Accompagnement** : Séances de coaching pour les équipes IT et réunions régulières pour évaluer l'avancement.
   - **Formation** : Sessions de formation pratiques sur la mise en œuvre des changements.
3. **Analyse de Résultat**
   - **Gestion CDC** : Analyse détaillée des résultats du pilote et ajustements basés sur les feedbacks.
   - **Accompagnement** : Débriefings avec les équipes pour discuter des résultats et des améliorations.
4. **Validation**
   - **Gestion CDC** : Validation finale de la conformité avec la directive NIS 2 et résolution des dernières résistances et défis.
   - **Accompagnement** : Préparation pour l'audit de conformité NIS 2.
5. **Lancement**
   - **Gestion CDC** : Lancement officiel des nouvelles pratiques de cybersécurité et mise en place de la surveillance continue pour évaluer les performances.
   - **Accompagnement** : Support continu pour les équipes.
   - **Communication** : Annonce de la réussite de la mise en conformité.
   - **Formation** : Cycles de formation continue sur les mises à jour de la directive NIS 2 et les meilleures pratiques en cybersécurité.

La mise en œuvre de ce plan est cruciale pour garantir que les entreprises répondent aux exigences de la directive NIS 2, ce qui contribue à améliorer la sécurité et la résilience de leurs infrastructures critiques. En suivant ce plan, les entreprises peuvent systématiquement évaluer et renforcer leurs mesures de sécurité, réduire les risques de cyberattaques, et assurer la continuité des opérations. De plus, ce plan facilite une transition en douceur vers la conformité, minimise les résistances au changement et assure un soutien continu pour les équipes impliquées, renforçant ainsi la culture de la cybersécurité au sein de l'organisation.

4.8.2 Le modèle de formation

Pour accompagner le changement, les entreprises peuvent également s’aider de plusieurs autres modèles dont:

Le modèle de formation (figure 41) qui permet de planifier, structurer et détailler les formations qui vont avoir lieu. Ce modèle joue un rôle crucial dans la préparation des équipes à adopter de nouvelles pratiques, technologies, ou régulations.

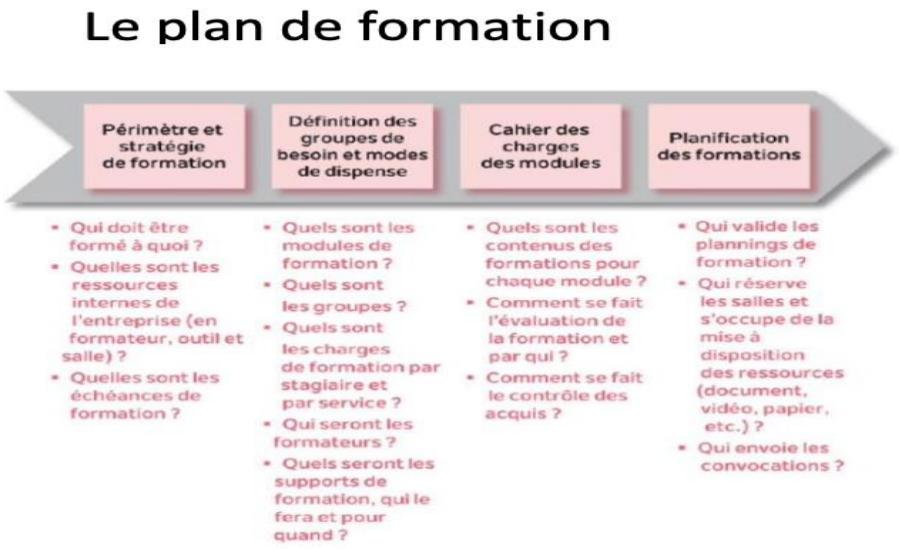


Figure 41: Plan de formation

Autissier, D., & Al. (2019). Outil 36. *Le plan de communication.* cairn.info. https://www.cairn.info/la-boite-a-outils-de-la-conduite-du-changement--9782100776344-page-108.htm

3.8.3 Le plan de transition

Le plan de transition (figure 42) qui fait office de plan d'action sur l'accompagnement du changement et qui se fait à la fin de la phase de l'étude d'impact.

PROCESSUS...						
Cible / Objectifs	Action 1...					
	Tâches	Criticité	Planning	Responsable	Participants	Livrables
	Action 2...					
	Tâches	Criticité	Planning	Responsable	Participants	Livrables
	-.....					
	-.....					
	-.....					
	-.....					
	-.....					
	Action 3...					
	Tâches	Criticité	Planning	Responsable	Participants	Livrables
	-.....					
	-.....					
	-.....					
	-.....					
	-.....					

Figure 42: Plan de transition

Autissier, D., & Al. (2019). Outil 36. *Le plan de communication.* cairn.info. https://www.cairn.info/la-boite-a-outils-de-la-conduite-du-changement--9782100776344-page-108.htm

4.8.4 Le baromètre ICAP

Le baromètre ICAP est un outil utilisé pour mesurer et suivre la progression de l'acceptation et de l'engagement des employés lors d'un projet de changement dans une organisation à partir de 4 taux : l'information, la compréhension, l'adhésion et la participation des destinataires du changement.

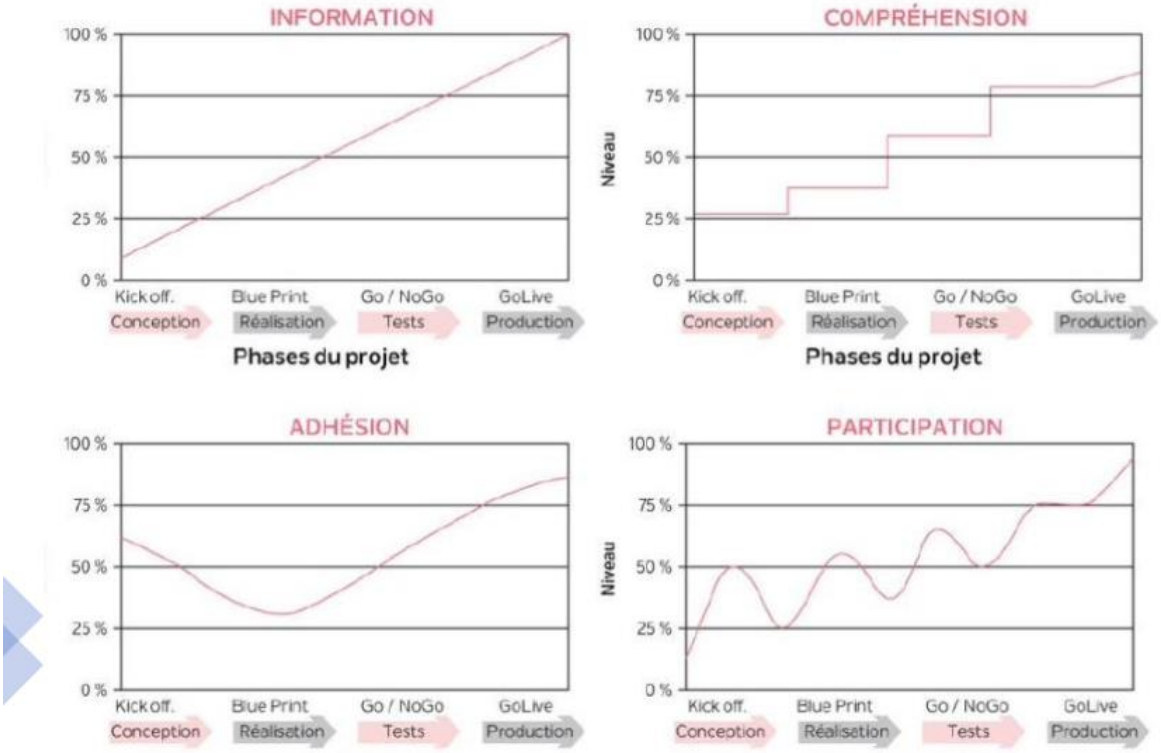


Figure 43: Le baromètre ICAP

Autissier, D., & Al. (2019). Outil 36. *Le plan de communication.* cairn.info. https://www.cairn.info/la-boite-a-outils-de-la-conduite-du-changement--9782100776344-page-108.htm

La figure ci-dessus illustre un exemple de graphiques typiquement utilisés pour représenter les données recueillies par le baromètre ICAP au cours des différentes phases d'un projet de changement. Chaque graphique montre l'évolution de l'un des quatre critères (Information, Compréhension, Adhésion, et Participation) à travers les différentes étapes du projet.

Bien que l'exemple présenté dans l'image soit spécifique à un projet, il est important de noter que tous les baromètres ICAP ne se ressemblent pas nécessairement. La forme et la nature des données peuvent varier selon les spécificités du projet, la culture de l'entreprise, les méthodes de mesure utilisées, et l'engagement des employés. Certains projets pourraient montrer une progression plus stable dans certaines dimensions, tandis que d'autres pourraient connaître des fluctuations plus marquées.

Pour générer ces graphiques, il faut suivre plusieurs étapes :

1) Création du questionnaire

2) Réalisation des enquêtes et calcul des taux
3) Évaluation des indicateurs

4.9 Actions à mettre en place

Dans l'article 21 de la directive sont reprises les mesures de gestion des risques en matière de cybersécurité que les entités concernées par la directive NIS 2 doivent respecter pour se conformer. Lors de mes recherches sur le terrain auprès d'Agoria, j'avais pour mission de faire la correspondance entre chacune des mesures de la directive et les actions proposées par le Framework du CCB.
Il se trouve que le CCB propose une centaine de contrôles dans son Framework, ici je vais reprendre que quelques-uns que je trouve pertinents. La liste n'est pas exhaustive et d'autres actions peuvent être proposées ou entreprises pour chaque mesure de la directive. Il faudra alors se rediriger vers le document du CCB avec la liste complète des actions qui est accessible gratuitement.
En effet, si on applique toutes les mesures proposées par la directive, on est conforme. Cependant, étant donné que la transposition de la directive en législation nationale n'a pas encore été adoptée dans tous les pays, il peut y avoir un délai avant que les actions exactes à mettre en place soient définies clairement cela n'empêche pas pour autant les entités de commencer à agir pour renforcer leur cybersécurité dès maintenant, car les mesures de la directive reflètent généralement les meilleures pratiques en matière de cybersécurité. (Vanden Geeten, 2024)

PDCA :

La roue de Deming, ou cycle PDCA (Plan-Do-Check-Act), est un outil essentiel pour l'implémentation de systèmes de gestion qui nécessitent une amélioration continue, dans le cadre de la directive NIS 2 concernant la cybersécurité. Ce modèle est particulièrement pertinent pour les entités qui doivent intégrer des mesures strictes de gestion des risques en matière de cybersécurité telles que celles stipulées dans l'article 21.

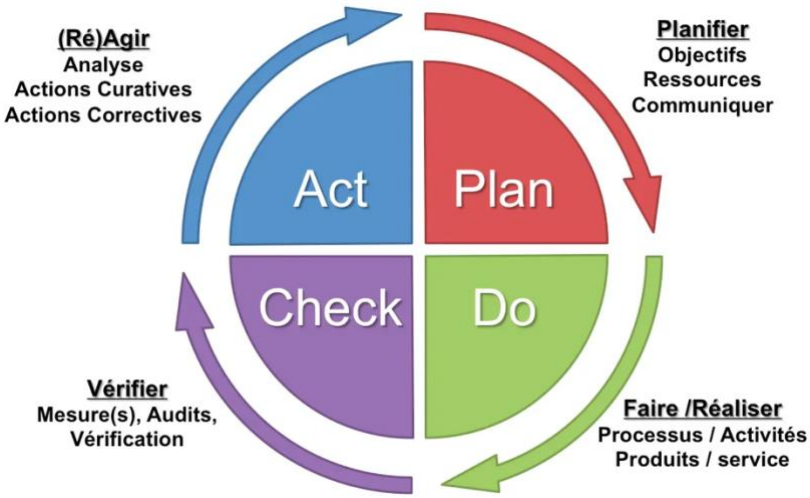


Figure 44 : Modèle PDCA
C-Qse. (2019, 6 novembre). *Cycle PDCA / La roue de Deming.* Certification QSE. Consulté le 20 avril 2024, à l'adresse https://www.certification-qse.com/cycle-pdca-roue-de-deming/

Dans l'annexe 4, vous trouverez une liste des actions proposées pour chaque mesure de la directive NIS 2 en matière de cybersécurité. Cette liste comprend une sélection d'actions pertinentes qui peuvent être mises en œuvre par les entités concernées pour se conformer aux exigences de la directive. Cette liste vient de ma propre initiative, où lors de mon stage, j'ai eu la tâche d'analyser le framework de la CCB et de tirer les actions qu'il propose correspondant à la mesure adéquate.

En mettant en œuvre les actions situé dans l'annexe 4, les entreprises amorceront de manière significative leur chemin vers la conformité avec la directive NIS 2. Il est important de noter que bien que la directive n'ait pas encore été complètement transposée en législation nationale dans tous les pays, et que les actions spécifiques à mettre en place restent à préciser, l'initiative de renforcer la cybersécurité conformément à cette directive constitue un pas prudent et proactif. Cela dit, la mise en œuvre des mesures suggérées ici ne suffira pas à elle seule pour garantir une conformité totale une fois que la législation sera en place. Les spécificités sectorielles manquent et d'autres actions pourraient être requises. L'objectif de ce chapitre était de fournir une vue d'ensemble des mesures essentielles et d'initier les démarches pour leur mise en œuvre. Pour une compréhension exhaustive et des actions détaillées, il est conseillé de consulter le document du CCB qui offre une liste complète des contrôles disponibles gratuitement. En anticipant et en appliquant ces pratiques recommandées, l'organisation se positionnera avantageusement pour répondre aux exigences futures et renforcer sa posture globale de cybersécurité.

4.10 Conclusion intermédiaire

L'analyse empirique menée dans cette section a mis en lumière les défis et opportunités associés à la mise en œuvre de la directive NIS 2. Elle a révélé que le changement nécessaire pour se conformer à cette directive n'est pas seulement technologique mais également organisationnel.

Il est apparu que le succès de l'implémentation de la directive dépend largement de la compréhension profonde et de l'alignement stratégique de l'organisation avec les exigences de NIS 2. Les entreprises doivent adapter leurs structures internes et leurs processus pour intégrer les nouvelles exigences de manière fluide. L'alignement stratégique implique de faire comprendre à tous les niveaux de l'organisation l'importance de la cybersécurité et de la conformité réglementaire.

La gestion du changement émerge comme une composante essentielle. Les entretiens avec des experts ont souligné que le changement ne doit pas être perçu uniquement comme une contrainte mais comme une opportunité de renforcer la résilience et la sécurité organisationnelle. La communication joue un rôle crucial : des plans de communication détaillés et des outils de communication variés (comme le mix com) permettent d'informer et de sensibiliser efficacement toutes les parties prenantes. La co-construction du changement, impliquant activement les employés dans le processus, favorise l'acceptation et l'adhésion aux nouvelles pratiques.

Les ressources humaines sont au cœur de la réussite de la mise en œuvre de la directive NIS 2. Il est impératif de former continuellement le personnel à la cybersécurité, en utilisant des programmes de formation adaptés et actualisés. Les entretiens ont également mis en évidence la nécessité d'avoir des leaders et des experts en cybersécurité pour piloter ces initiatives.

L'analyse a montré que l'intégration des technologies avancées et la mise en place de processus robustes sont essentielles pour répondre aux exigences de NIS 2. L'utilisation de systèmes d'authentification multifactorielle, de communications sécurisées, et de gestion des incidents fait partie des mesures clés à adopter. Les processus doivent être régulièrement audités et améliorés pour maintenir un haut niveau de sécurité.

L'un des principaux enseignements de cette section est que la directive NIS 2, bien qu'imposant des défis significatifs, offre également des opportunités de renforcer la résilience organisationnelle et d'améliorer la crédibilité et la confiance des clients. En se conformant à cette directive, les organisations peuvent non seulement réduire leurs risques de cybersécurité mais aussi valoriser leur position sur le marché numérique.

En conclusion, cette analyse empirique fournit des insights précieux et des recommandations pratiques pour aider les entreprises à naviguer dans le paysage complexe de la conformité à la directive NIS 2. Elle souligne l'importance d'une approche holistique intégrant la stratégie, la communication, la technologie, et la formation pour transformer les défis de la cybersécurité en opportunités de croissance et d'innovation durable.

Section 5 : Futur work, contribution recommandations et conclusions.

5.1 Introduction

Tout au long de ce mémoire, ainsi qu'à travers les diverses interviews menées, plusieurs problématiques cruciales ont été soulevées concernant la mise en œuvre de la directive NIS 2 et la cybersécurité en Belgique. Ces problématiques touchent à la complexité administrative, au manque de ressources et de compétences en cybersécurité, aux différences sectorielles, aux défis de collaboration internationale, et au rôle des autorités de contrôle.

Ces défis révèlent la nécessité d'une approche holistique et coordonnée pour renforcer la résilience cybernétique des entreprises belges. La directive NIS 2, en élargissant son champ d'application et en introduisant des exigences plus strictes, agit comme un catalyseur pour l'amélioration de la cybersécurité. Cependant, pour que cette directive soit efficace, il est essentiel d'adopter des stratégies qui répondent de manière pragmatique et ciblée aux problématiques identifiées.

Dans cette section, je vais détailler les principales problématiques identifiées lors des interviews avec des experts en cybersécurité et proposer des recommandations concrètes pour y remédier. Ces recommandations visent à simplifier les procédures administratives, à renforcer les capacités des entreprises en matière de cybersécurité, à harmoniser les exigences sectorielles, à améliorer la collaboration internationale, et à accroître l'efficacité des autorités de contrôle.

En abordant ces aspects, je pourrai offrir aux entreprises un cadre clair et des outils pratiques pour se conformer aux nouvelles normes de cybersécurité, tout en promouvant une culture de sécurité proactive. Cette démarche permettra non seulement de se conformer à la directive NIS 2, mais aussi de renforcer la résilience globale de l'écosystème numérique belge face aux menaces croissantes.

5.2 Problématiques

Cette section vise à identifier ces problématiques majeures des différentes interview et à proposer des recommandations par la suite pour y remédier. Les enjeux identifiés sont complexes et variés, touchant à la fois les aspects techniques, organisationnels et humains de la cybersécurité.

Problématiques soulevées :

Complexité et Charge Administrative : La directive NIS 2 impose des exigences élevées en matière de cybersécurité, entraînant une charge administrative accrue, particulièrement pour les petites et moyennes entreprises (PME). Cette complexité peut freiner la mise en conformité et augmenter les coûts opérationnels.

Différences Sectorielles : Les exigences en matière de cybersécurité varient considérablement selon les secteurs, compliquant ainsi la mise en conformité. Chaque secteur ayant ses spécificités, les mesures de sécurité doivent être adaptées en conséquence, ce qui nécessite une compréhension approfondie et des actions ciblées.

Collaboration Internationale : La directive NIS 2 a des implications qui s'étendent au-delà des frontières de l'UE, rendant la collaboration internationale essentielle mais complexe. La gestion des fournisseurs internationaux et l'assurance de leur conformité aux normes européennes ajoutent une couche supplémentaire de difficulté.

Pénurie de Talents en Cybersécurité : Un des défis majeurs est le manque de professionnels qualifiés pour répondre à la demande croissante en cybersécurité. Cette pénurie exacerbe les difficultés rencontrées par les entreprises pour se conformer aux nouvelles réglementations. Les PME, en particulier, peinent à recruter et à retenir des experts en cybersécurité en raison de contraintes budgétaires.

Sensibilisation et Formation : Il y a un besoin urgent de sensibilisation accrue à la cybersécurité et de programmes de formation à tous les niveaux organisationnels, y compris pour la haute direction et les membres des conseils d'administration. Assurer que les employés de différents départements, pas seulement ceux de l'informatique, comprennent et respectent les politiques de cybersécurité est crucial. Il y a une prise de conscience insuffisante au sein des conseils d'administration et des équipes de direction sur les responsabilités et les implications de la directive NIS 2. Beaucoup de dirigeants ne comprennent pas pleinement les risques et les obligations liés à la cybersécurité.

Sécurité de la Chaîne d'Approvisionnement : La nécessité de sécuriser la chaîne d'approvisionnement est essentielle, en particulier avec des fournisseurs non directement couverts par la directive NIS 2 mais critiques pour les opérations des entités conformes. Aborder les obligations contractuelles et de conformité des fournisseurs internationaux est également une priorité.

Soutien aux Petites et Moyennes Entreprises (PME) : Les difficultés rencontrées par les PME pour répondre aux nouvelles exigences en matière de cybersécurité sont amplifiées par leurs ressources et expertises limitées. Il est crucial de fournir des outils accessibles, des conseils et un soutien financier pour aider les PME dans leurs efforts de conformité. La mise en conformité avec la directive NIS 2 peut être coûteuse, particulièrement pour eux qui n'ont pas les mêmes ressources que les grandes entreprises.

Les coûts liés à l'embauche de consultants externes et à l'achat de technologies de cybersécurité peuvent être prohibitifs.

Hétérogénéité des Pratiques de Cybersécurité et Manque de Standardisation : Les pratiques de cybersécurité varient considérablement d'une entreprise à l'autre et d'un secteur à l'autre, ce qui complique la mise en conformité avec des standards uniformes comme ceux de la directive NIS 2.

Complexité de la Communication Interne sur les Politiques de Cybersécurité : La mise en œuvre de politiques de cybersécurité nécessite une communication efficace entre les différents départements d'une entreprise. Cependant, il est souvent difficile d'assurer une diffusion homogène des informations et des directives à tous les niveaux de l'organisation.

5.3 Recommandations

En identifiant et en analysant ces problématiques, ce mémoire propose des recommandations pour aider les entreprises à surmonter ces défis et à améliorer leur résilience en matière de cybersécurité. Les voici :

Simplification et Standardisation des Procédures :

- **Recommandation** : Développer des outils standardisés et accessibles pour aider les entreprises à se conformer à la directive NIS 2, notamment des guides pratiques et des checklists.
- **Action** : Le Centre pour la Cybersécurité Belgique (CCB) pourrait créer une plateforme centralisée avec des ressources gratuites et des modèles de conformité.

Renforcement des Capacités et Mutualisation des Ressources :

- **Recommandation** : Encourager la mutualisation des ressources en cybersécurité, par exemple en permettant à plusieurs PME de partager les services d'un consultant en cybersécurité.
- **Action** : Mettre en place des subventions et des aides publiques pour soutenir les initiatives de mutualisation. Il existe déjà certaines subventions et aides, il faudrait alors faire un travail de communication dessus et les faire connaitre.

Formation et Développement des Compétences :

- **Recommandation** : Investir dans la formation continue des professionnels de la cybersécurité et offrir des programmes de formation spécifiques pour les PME.
- **Action** :
  - Créer des partenariats avec des institutions académiques et des organisations professionnelles pour offrir des formations adaptées aux besoins du marché.
  - Créer une plateforme pour faire un matche entre les poste vacant et les professionnelles à la recherche d'un emploi pour le milieu de la cyber.

Harmonisation des Exigences Sectorielles :

- **Recommandation** : Développer des cadres de sécurité sectoriels qui complètent les exigences générales de la directive NIS 2.

- **Action** : Collaborer avec les autorités sectorielles pour définir des mesures spécifiques et des lignes directrices claires.

Amélioration de la Collaboration Internationale :

- **Recommandation** : Établir des accords bilatéraux et multilatéraux pour faciliter la conformité des fournisseurs internationaux aux normes européennes.
- **Action** : Travailler avec les institutions de l'UE pour harmoniser les exigences de cybersécurité au niveau global.

Soutien aux Petites et Moyennes Entreprises (PME) :

- **Recommandation** : Fournir des incitations financières et des subventions aux PME pour investir dans des mesures de cybersécurité.
- **Action** : Créer une plateforme centralisée offrant des ressources, des outils et des services de conseil spécialement conçus pour les besoins des PME.

Simplification des Processus de Certification :

- **Recommandation** : Développer un processus de certification rationalisé qui soit à la fois rigoureux et accessible, permettant aux organisations de démontrer facilement leur conformité.
- **Action** : Promouvoir l'adoption de cadres et de normes de cybersécurité unifiés, réduisant la complexité et favorisant la cohérence entre les secteurs.

5.4 Conclusion Générale

La directive NIS 2 a été une aubaine pour la sécurité des entreprises tant au niveau national qu'européen, apportant une nouvelle dimension à la gestion des risques en cybersécurité. Elle offre un cadre structuré et rigoureux pour renforcer les défenses des entités contre les cybermenaces croissantes. En mettant en place des mesures harmonisées et en encourageant une coopération transfrontalière, la directive NIS 2 contribue à élever le niveau de résilience et de sécurité numérique au sein de l'Union européenne. Cette initiative proactive est essentielle pour protéger les infrastructures critiques, les données sensibles et les opérations commerciales des entreprises, tout en favorisant un environnement numérique plus sûr et plus fiable pour tous.

Ce mémoire a exploré en profondeur les moyens par lesquels les entreprises peuvent se conformer à cette directive NIS 2 et promouvoir une culture robuste de cybersécurité, en prenant le cas d'Agoria comme exemple illustratif. La directive NIS 2, en tant que cadre réglementaire crucial, vise à renforcer la résilience des réseaux et des systèmes d'information au sein de l'Union européenne, répondant ainsi à l'augmentation des cybermenaces et à la complexité croissante de la cybersécurité.

Le contexte de la directive NIS 2 est marqué par une montée en puissance des cyberattaques telles que le ransomware, le phishing et les attaques DDoS. Ces menaces non seulement compromettent la sécurité des informations sensibles mais perturbent également les opérations critiques des organisations. La Belgique, en tant que centre névralgique politique et économique de l'Europe, est particulièrement vulnérable à ces menaces. Par conséquent, la directive NIS 2 représente une réponse essentielle pour accroître la vigilance et la préparation face à ces défis.

Le mémoire utilise une approche méthodologique mixte, combinant des analyses de concepts théoriques et des entretiens qualitatives pour évaluer l'état de préparation des entreprises à la conformité avec la directive NIS 2. L'étude de cas d'Agoria, la fédération de la technologie en Belgique, a révélé les initiatives prises pour sensibiliser et accompagner les entreprises dans cette transition réglementaire. Des entretiens avec des experts du domaine ont fourni des insights précieux sur les défis et les meilleures pratiques en matière de mise en œuvre de la directive.

La conformité à la directive NIS 2 ne doit pas seulement être vue comme une obligation, mais aussi comme une opportunité pour les entreprises d'améliorer leur position sur le marché. En adoptant des mesures de cybersécurité robustes, les entreprises peuvent gagner en crédibilité et en confiance auprès de leurs clients et partenaires commerciaux. De plus, la mise en place de systèmes de sécurité avancés peut faciliter l'innovation en permettant aux entreprises d'explorer de nouvelles technologies et méthodes pour protéger leurs données et systèmes. Cette dynamique positive peut conduire à une croissance soutenue et à une meilleure compétitivité sur le marché global.

Un des éléments clés pour une cybersécurité efficace est la collaboration. Encourager la collaboration entre les différents secteurs, ainsi que le partage d'informations sur les cybermenaces et les meilleures pratiques de sécurité, est crucial. Les entreprises doivent être prêtes à travailler ensemble, à partager leurs expériences et à apprendre les unes des autres pour renforcer la résilience collective contre les cyberattaques. Cette approche collaborative peut aider à identifier rapidement les menaces émergentes et à développer des stratégies de réponse plus efficaces.

La cybersécurité est un domaine en constante évolution, avec de nouvelles menaces et technologies qui apparaissent régulièrement. Il est donc essentiel de mettre l'accent sur la formation continue pour les professionnels de la cybersécurité afin de maintenir des compétences à jour. Les entreprises doivent investir dans des programmes de formation réguliers pour leurs employés, en couvrant non seulement les aspects techniques, mais aussi les aspects stratégiques et opérationnels de la cybersécurité. Une main-d'œuvre bien formée est une ligne de défense cruciale contre les cybermenaces.

Les petites et moyennes entreprises (PME) doivent également être encouragées à adopter des mesures de cybersécurité proportionnées à leurs capacités. Il est important de sensibiliser ces entreprises aux avantages de la conformité à la directive NIS 2 et de leur fournir les ressources nécessaires pour mettre en œuvre des pratiques de sécurité efficaces. Cela peut inclure des subventions, des incitations financières, et un accès facilité à des formations et des outils de sécurité. En soutenant les PME, on renforce l'ensemble de l'écosystème économique contre les cybermenaces.

L'analyse a montré que, bien que les entreprises commencent à reconnaitre l'importance de la cybersécurité, elles sont souvent confrontées à des obstacles significatifs, tels que la complexité technique, le coût élevé des mesures de sécurité et le manque de compétences spécialisées. Agoria joue un rôle crucial en fournissant des ressources, des formations et des conseils stratégiques pour aider ses membres à naviguer dans ce paysage réglementaire complexe.

Pour promouvoir une conformité efficace à la directive NIS 2, il est recommandé que les organisations adoptent une approche proactive de la gestion des risques en cybersécurité, intégrant des processus robustes de détection et de réponse aux incidents. Il est également essentiel de renforcer la formation et la sensibilisation des employés pour réduire les erreurs humaines, qui sont une cause majeure des violations de sécurité.

En conclusion, la directive NIS 2 est un cadre essentiel pour améliorer la résilience des systèmes d'information en Europe. La mise en œuvre réussie de cette directive nécessite une collaboration étroite entre les régulateurs, les fédérations industrielles comme Agoria et les entreprises elles-mêmes. En adoptant des stratégies de cybersécurité robustes et en renforçant leur culture de sécurité, les organisations peuvent non seulement se conformer aux exigences réglementaires mais aussi renforcer leur positionnement dans l'économie numérique globale. Ce mémoire offre un cadre analytique et des recommandations pratiques pour aider les entreprises à transformer les défis de la cybersécurité en opportunités de croissance et d'innovation.

Bibliographie

Agoria. (s. d.). *À propos de nous*. Consulté le 20 mars 2024, à l'adresse https://www.agoria.be/fr/a-propos-de-nous

Agoria. (2022, novembre) *gouvernance CMiB* [Présentation Power Point]. Agoria

Altospam. (s.d.). *Qu'est-ce qu'un ransomware ? Comment se protéger des ransomwares ?* Altospam. Consulté le 12 octobre 2023, à l'adresse https://www.altospam.com/glossaire/ransomware/

Alonso, C. (2022, 5 septembre). *Qu'est-ce que le modèle COSO ? Comment gérer les risques.* GlobalSuite Solutions. Consulté le 9 février 2024, à l'adresse https://www.globalsuitesolutions.com/fr/que-est-ce-que-le-modele-coso-gerer-les-risques/

AON. (2023, octobre). *Rapport 2023 sur la cyberrésilience*. Consulté le 12 février 2024, à l'adresse https://www.aon.com/2023-cyber-resilience-report/fr

Atlassian. (s. d.). *Gestion des incidents : processus, bonnes pratiques et outils*. Consulté le 27 mars 2024, à l'adresse https://www.atlassian.com/fr/incident-management#the-importance-of-incident-management

Autissier, D., & Al. (2018). *Conduite du changement : concepts clés (3e éd.).* Dunod. https://www.dunod.com/sites/default/files/atoms/files/9782100769414/Feuilletage.pdf

Autissier, D., & Al. (2019). *Outil 36. Le plan de communication.* Dunod ; cairn.info. https://www.cairn.info/la-boite-a-outils-de-la-conduite-du-changement--9782100776344-page-108.htm

Autissier, D., Vandangeon-Derumez, I., Vas, A., & Johnson, K. P. (2018). *Chapitre 19. Céline Bareil et André Savoie*. Dunod

Autissier, D., Moutot, J. M., & Charbonnier, O. (2010). *Le changement organisationnel : Théories et Pratiques.* Dunod

Autorité de protection des données. (s. d.). *Sanctions*. Consulté le 10 octobre 2023, à l'adresse https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/delegue-a-la-protection-des-donnees/sanctions-

Autorité de protection des données. (s. d.). *Une politique de sécurité de l'information*. Consulté le 10 octobre 2023, à l'adresse https://www.autoriteprotectiondonnees.be/professionnel/themes/securite-de-l-information/une-politique-de-securite-de-linformation

Bannister, A. (2019, 9 décembre). *When the screens went black: How NotPetya taught Maersk to rely on resilience – not luck – to mitigate future cyber-attacks.* PortSwigger. Consulté le 28 avril 2024, à l'adresse https://portswigger.net/daily-swig/when-the-screens-went-black-how-notpetya-taught-maersk-to-rely-on-resilience-not-luck-to-mitigate-future-cyber-attacks

Banque de développement du Canada. (2023, 29 mai). *Comment la certification ISO 27001 peut aider à sécuriser l'information de votre entreprise.* Consulté le 16 octobre 2023, à l'adresse https://www.bdc.ca/fr/articles-outils/operations/iso-autres-certifications/comment-certification-iso-peut-aider-securiser-information-votre-entreprise

Batsleer, P., & Debuisson, A. (2024, 13 mai). *Consultants cybersécurité*, Nviso [Entretien]. Teams.

Bergé, J. (2021, 20 juillet). *La gestion des risques, gage de survie au XXIe siècle - Harvard Business Review* France. HBR France. Consulté le 12 février 2024, à l'adresse https://www.hbrfrance.fr/chroniques-experts/2021/07/37227-la-gestion-des-risques-gage-de-survie-au-xxie-siecle/

Bonneaud, A. (2019, 4 mars). *Guide COBIT 2019 : de A jusqu'à Z*. Blog de la Transformation Digitale. Consulté le 2 avril 2024, à l'adresse https://www.ab-consulting.fr/blog/cobit-2019/guide-cobit-2019-de-a-jusqua-z

Bouche, T.-J. (2020, 27 janvier). *Donnée à caractère personnel : Qu'est ce que c'est ?.* DPO Expert. Consulté le 20 octobre 2023, à l'adresse https://dpoexpert.fr/donnee-a-caractere-personnel/

Bourgin, Y. (2024, 29 février). *Une cyberattaque perturbe fortement des pharmacies et hôpitaux, le gang BlackCat pointé du doigt.* Usine-digitale. Consulté le 24 avril 2024, à l'adresse https://www.usine-digitale.fr/article/une-cyberattaque-perturbe-fortement-des-pharmacies-et-hopitaux-le-gang-blackcat-pointe-du-doigt.N2209135

Byttebier, P. (2022, 30 avril). *NIS-2 : état des lieux*. Centre Pour la Cybersécurité Belgique. Consulté le 19 février 2024, à l'adresse https://ccb.belgium.be/fr/actualit%C3%A9/nis-2-%C3%A9tat-des-lieux

C-Qse. (2019, 6 novembre). *Cycle PDCA / La roue de Deming*. Certification QSE. Consulté le 20 avril 2024, à l'adresse https://www.certification-qse.com/cycle-pdca-roue-de-deming/

Capano, D. E. (2023, 29 décembre). *Throwback attack : How NotPetya ransomware took down Maersk. Industrial Cybersecurity* Pulse. Consulté le 28 avril 2024, à l'adresse https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

CCB. (2016). *Cybersécurité : Stratégie et Guide [PDF]*. Consulté le 10 mars 2024, à l'adresse https://ccb.belgium.be/sites/default/files/CSIMG_2016_FR.pdf

CCB. (2022, 2 septembre). *Comment répondre à une attaque par ransomware en 12 étapes*. Consulté le 14 février 2024, à l'adresse https://ccb.belgium.be/fr/document/comment-r%C3%A9pondre-%C3%A0-une-attaque-par-ransomware-en-12-%C3%A9tapes

CCB. (2023, 24 mars). *Centre for Cybersecurity Belgium launches security standards to boost cybersecurity in companies and organisations.* Consulté le 13 mars 2024, à l'adresse https://ccb.belgium.be/en/news/centre-cybersecurity-belgium-launches-security-standards-boost-cybersecurity-companies-and

CCB. (2023, juin) *NIS 2 in BE* [Présentation Power Point]. CCB

CCB. (2024, 11 janvier). *Projets et cybermenaces : CCB rapport 2023.* Centre Pour la Cybersécurité Belgique. https://ccb.belgium.be/fr/actualit%C3%A9/projets-et-cybermenaces-ccb-rapport-2023

CCB. (2024, 29 janvier). *Rapport annuel 2023. Centre Pour la Cybersécurité Belgique*. Consulté le 13 mars 2024, à l'adresse https://ccb.belgium.be/fr/actualit%C3%A9/rapport-annuel-2023

CCB. (2024, 9 avril). *La directive NIS2 : que cela signifie-il pour mon organisation ?* Consulté le 19 avril 2024, à l'adresse https://ccb.belgium.be/fr/la-directive-nis2-que-cela-signifie-il-pour-mon-organisation

CCB SafeOnWeb. (s. d.). *CyberFundamentals Framework*. Consulté le 14 février 2024, à l'adresse https://atwork.safeonweb.be/fr/tools-resources/cyberfundamentals-framework

Centre de Crise National. (s. d.). *Cyber-criminalité*. Consulté le 14 février 2024, à l'adresse https://centredecrise.be/fr/risques-en-belgique/risques-pour-la-securite/cyber-criminalite

CNIL. (2016). *Le règlement général sur la protection des données - RGPD.* Consulté le 4 novembre 2024, à l'adresse https://www.cnil.fr/fr/reglement-europeen-protection-donnees

CNIL. (2018). *CNIL guide sécurité personnelle*. Consulté le 4 novembre 2023, à l'adresse www.cnil.fr: https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

Cobb, M. (2023, 15 août). *ISO 31000 vs. COSO: Comparing risk management standards.* TechTarget CIO. Consulté le 15 février 2024, à l'adresse https://www.techtarget.com/searchcio/feature/ISO-31000-vs-COSO-Comparing-risk-management-standards

Commission européenne. (s.d.-a). *À quoi correspondent les données à caractère personnel?* Consulté le 17 octobre 2023, à l'adresse https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_fr

Commission européenne. (s. d.-b). *Cybersecurity Strategy*. Consulté le 19 février 2024, à l'adresse https://digital-strategy.ec.europa.eu/fr/policies/cybersecurity-strategy

Commission Européenne. (s. d.-c). *Que se passe-t-il si mon entreprise/organisation ne respecte pas les règles en matière de protection des données ?* Consulté le 13 février 2024, à l'adresse https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_fr#:~:text=violation%3A%20les%20sanctions%20comprennent%20un,mondial%20total%20de%20l%27entreprise

Commission européenne. (2020). *Cyber Resilience Act*. Consulté le 23 avril 2024, à l'adresse https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Commission européenne. (2024, 8 mars). *AI Office*. Consulté le 14 février 2024, à l'adresse https://digital-strategy.ec.europa.eu/en/policies/ai-office

CustUp, L. (2023). *L'essentiel à connaître sur le RGPD : définition, périmètre, principes et mesures.* CustUp. Consulté le 10 octobre 2023, à l'adresse https://www.custup.com/introduction-gdpr-rgpd/

Cybermalveillance.gouv.fr. (2019, 9 octobre). *Attaque en déni de service (DDoS)*. Consulté le 10 octobre 2023, à l'adresse https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service ddos#:~:text=Une%20attaque%20en%20déni%20de,fonctionnement%20fortement%20dégradé%20du%20service.

Cyber Security Coalition. (2021, 31 mars). *EU Cybersecurity Act : moving forward - Cyber Security Coalition.*
Consulté le 23 avril 2024, à l'adresse https://www.cybersecuritycoalition.be/fr/eu-cybersecurity-act/

Data Legal Drive. (2023, 28 juin). *Directive NIS2 & RGPD : Renforcement de protection des données ?* Consulté le 15 février 2024, à l'adresse https://datalegaldrive.com/directive-nis2-rgpd-renforcement-de-protection-des-donnees/

David, B. (2021, 8 décembre). *The Impact of Emerging Technology on the Future of Cybersecurity*. Infosecurity Magazine.
https://www.infosecurity-magazine.com/magazine-features/emerging-technology-future/

Dèbes, F. (2018, 25 mai). *Protection des données personnelles : Quand l'Europe inspire le monde.* Les Echos.
https://www.lesechos.fr/tech-medias/hightech/protection-des-donnees-personnelles-quand-leurope-inspire-le-monde-132849

De Kerchove, F. (2024, 2 mai). *Lobby et advocacy pour le digital* [Entretien]. Teams.

Deloitte. (2016). *Gestion des risques liés aux technologies de l'information (TI).* Consulté le 16 octobre 2023, à l'adresse https://www2.deloitte.com/ch/fr/pages/risk/articles/it-risk-management.html

Direction du Système d'Information et des Usages Numériques. (2020, 29 septembre). *La Sécurité du Système d'Information (SSI)*. Consulté le 20 novembre 2023, à l'adresse https://dsiun.univ-tln.fr/La-Securite-du-Systeme-d-Information-SSI.html

Ejzyn, A., & Van den Berghe, T. (2019). *Cybersécurité et RGPD : protégez votre PME. Guide pratique pour sécuriser votre système informatique et vous conformer au RGPD*. Legitech.

European Cyber Resilience Act. (2022). *The European Cyber Resilience Act*. Consulté le 23 avril 2024, à l'adresse https://www.european-cyber-resilience-act.com/#:~:text=The%20European%20Cyber%20Resilience%20Act%20is%20a%20legal%20framework%20that,throughout%20a%20product's%20life%20cycle.

European Data Protection Supervisor. (s. d.). *Sécurité de l'information*. Consulté le 2 octobre 2023, à l'adresse https://edps.europa.eu/data-protection/data-protection/reference-library/information-security_fr

European Securities and Markets Authority. (2023, juin). *DORA Public Consultation Overview Document*. Consulté le 10 avril 2024, à l'adresse https://www.esma.europa.eu/sites/default/files/2023-06/DORA_public_consultation_overview_document.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.esma.europa.eu%2Fsites%2Fdefault%2Ffiles%2F2023

European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023: July 2022 to June 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Feel Agile. (2023, 5 octobre). *Norme ISO 27001 - Comprendre les exigences - Feel agile*. Consulté le 18 ocotbre 2023, à l'adresse https://feelagile.com/certification-iso-27001/

Féraud-Courtin, M., & Flambard, G. (2017, 22 novembre). *RGPD : les 6 étapes de la conformité*. Deloitte Société D'Avocats. Consulté le 15 février 2024, à l'adresse https://blog.avocats.deloitte.fr/rgpd-6-etapes-de-conformite/

Figaro. (2022, 10 mai). *La cybercriminalité a coûté plus de 6000 milliards de dollars en 2021*. Le Figaro. Consulté le 23 novembre 2023, à l'adresse https://www.lefigaro.fr/secteur/high-tech/la-cybercriminalite-a-coute-plus-de-6000-milliards-de-dollars-en-2021-20220510

Filippone, D. (2023, 10 octobre). *Les attaques par ransomware plus rapides que jamais.* LeMondeInformatique. Consulté le 20 octobre 2023, à l'adresse https://www.lemondeinformatique.fr/actualites/lire-les-attaques-par-ransomware-plus-rapides-que-jamais-91812.html

Foltýn, T. (2018, 2 mars). *GitHub knocked briefly offline by biggest DDoS attack ever*. We Live Security. Consulté le 20 avril 2024, à l'adresse https://www.welivesecurity.com/2018/03/02/github-knocked-briefly-offline-biggest-ddos-attack/

France, A. (2024, 6 janvier). *Ransomware cyber-attack on British Library 'set to cost £ 7m'*. Evening Standard. Consulté le 22 avril 2024, à l'adresse https://www.standard.co.uk/news/uk/ransomware-cyber-attack-british-library-cost-london-metropolitan-police-b1130718.html

Gastard, R. (2023, 9 novembre). *Cybersécurité : Qu'est-ce que la triade CIA ?* Jedha. Consulté le 20 novembre 2023, à l'adresse https://www.jedha.co/blog/cybersecurite-quest-ce-que-la-triade-cia

GDPR Info. (2016). *Sécurité du traitement - Article 32*. Consulté le 15 février 2024, à l'adresse https://gdprinfo.eu/fr/fr-article-32

Glaser, P. (2024, 19 mars). *NIS2, DORA et CRA : 3 mutations à venir dans le cyber*. INCYBER NEWS. Consulté le 23 avril 2024, à l'adresse https://incyber.org/article/nis2-dora-cra-mutations-cyber/

Global Suite Solutions. (2022, 22 décembre).. *Que sont les normes ISO ?* Consulté le 20 octobre 2023, à l'adresse https://www.globalsuitesolutions.com/fr/que-sont-les-normes-iso/#:~:text=Les%20normes%20ISO%20sont%20un,produits%20dans%20le%20secteur%20industriel

GlobalSuite Solutions. (2023, 28 décembre). *Qu'est-ce que la norme ISO 31000 et à quoi sert-elle ? Découvrez l'importance de la gestion des risques au sein de votre organisation.* Consulté le 13 février

2024, à l'adresse https://www.globalsuitesolutions.com/fr/quest-ce-que-la-norme-iso-31000-et-a-quoi-sert-elle/

Godart, F. S. N. (2017, 7 juillet). *Saint-Gobain, Mondelez et les autres chiffrent l'impact de la cyberattaque.* BFM BUSINESS. Consulté le 19 février 2024, à l'adresse https://www.bfmtv.com/economie/entreprises/services/saint-gobain-mondelez-et-les-autres-chiffrent-l-impact-de-la-cyberattaque_AN-201707070115.html

Grandmontagne, Y. (2017, 30 août). *Qu'est-ce que ITIL ? Les 5 meilleurs articles sur ITIL*. IT SOCIAL. Consulté le 27 mars 2024, à l'adresse https://itsocial.fr/enjeux-it/enjeux-production/it-service-management/quest-itil-5-meilleurs-articles-itil/

Hartley, T. (2024, 2 avril). *The Parkerian Hexad : Elevating Information Security Beyond the CIA Triad.* The Profit - Inspiring Business In Hawke's Bay. Consulté le 17 avril 2024, à l'adresse https://www.theprofit.co.nz/govern-tom-hartley-pro-tech/

Henderson, J.C., & Venkatraman, N. (1993). *Strategic alignment: Leveraging information technology for transforming organizations.* IBM Systems Journal, 32(1), 4-16.

Hurkadli, R. (2023, 31 août). *Framework COBIT 5.* ITSM Docs - ITSM Documents & Templates. Consulté le 20 mars 2024, à l'adresse https://www.itsm-docs.com/blogs/cobit/framework-cobit-5

IBM. (2022). *Qu'est-ce que le cadre de cybersécurité du NIST ?* Consulté le 24 avril 2024, à l'adresse https://www.ibm.com/fr-fr/topics/nist

IBM France News Room. (2023). *Rapport IBM : La moitié des organisations victimes d'une violation ne prévoient pas d'augmenter leurs dépenses de sécurité malgré la montée en flèche du coût des violations*. Consulté le 14 février 2024, à l'adresse https://fr.newsroom.ibm.com/Rapport-IBM-La-moitie-des-organisations-victimes-dune-violation-ne-prevoient-pas-daugmenter-leurs-depenses-de-securite-malgre-la-montee-en-fleche-du-cout-des-violations

Info Entrepreneurs. (2023, 1 octobre). *Gestion des risques*. Consulté le 12 février 2024, à l'adresse https://www.infoentrepreneurs.org/fr/guides/bl---gestion-des-risques/#1

Ionos. (2021, 24 août). *ITIL v4 : 4e édition du guide de la gestion des services informatiques.* IONOS Digital Guide. Consulté le 27 mars 2024, à l'adresse https://www.ionos.fr/digitalguide/web-marketing/vendre-sur-internet/quest-ce-quitil-v4/

Ironhack. (2023, 8 février). *Pourquoi la cybersécurité est-elle si importante ?* Consulté le 15 novembre 2023, à l'adresse https://www.ironhack.com/fr/blog/pourquoi-la-cybersecurite-est-elle-si-importante

ISO. (s. d.). *ISO - ISO 31000 — Management du risque*. Consulté le 12 février 2024, à l'adresse https://www.iso.org/fr/iso-31000-risk-management.html

ISO. (2022, 25 octobre). *ISO - La famille ISO/IEC 27000 — Management de la sécurité de l'information*. Consulté le 12 mars 2024, à l'adresse https://www.iso.org/fr/standard/iso-iec-27000-family

ISO. (2022, 1 mars). *ISO/IEC 27002 : 2022*. Consulté le 18 mars 2024, à l'adresse https://www.iso.org/fr/standard/75652.html

Kallenborn, G. (2018, 2 mars). *GitHub frappé par une attaque DDoS d'ampleur historique*. 01net. Consulté le 18 avril 2024, à l'adresse https://www.01net.com/actualites/github-frappe-par-une-attaque-ddos-d-ampleur-historique-1386567.html

Komnenic, M. (2024, 1 février). *61 biggest GDPR fines & penalties so far*. Termly. Consulté le 15 février 2024, à l'adresse https://termly.io/resources/articles/biggest-gdpr-fines/

KOUS, H. (2023, 15 août). *COSO ERM 2017 traduit en français [Diaporama]*. Consulté le 14 février 2024, à l'adresse https://fr.slideshare.net/hassanekoussoubeKOUS/coso-erm-2017-traduit-en-franaispdf

KPMG. (2020). *Maîtriser les risques liés aux technologies émergentes*. Consulté le 20 octobre 2023, à l'adresse https://assets.kpmg.com/content/dam/kpmg/fr/pdf/2020/01/fr-KPMG-ETR.pdf

Lexing. (2023, 16 novembre). *Directive NIS 2 : quels changements anticiper ?* Consulté le 19 février 2024, à l'adresse https://lexing.be/directive-nis-2-quels-changements-anticiper/

Marotte, S. (2022, 24 janvier). *La différence entre cybersécurité et sécurité de l'information.* Journal Du Net. Consulté le 15 novembre 2023, à l'adresse https://www.journaldunet.com/cybersecurite/1508277-la-difference-entre-cybersecurite-et-securite-de-l-information/

Marsh. (2022, octobre). *The Changing Face of Cyber Claims 2022*. Consulté le 29 novembre 2023, à l'adresse https://www.marsh.com/fr/fr/services/cyber-risk/insights/the-changing-face-of-cyber-claims-2022.html

Martin, A. (2023, 13 décembre). *Comment se mettre en conformité avec la Directive NIS 2 ?* Agoria. Consulté le 20 février 2024, à l'adresse https://www.agoria.be/fr/services/expertise/digitisation/cybersecurity/comment-se-mettre-en-conformite-avec-la-directive-nis-2

Martin, A. (2024, 2 avril). *Expert standardisation et légal chez Agoria* [Entretien]. Teams.

Ministry of Economic Affairs and Climate Policy. (2023, 20 octobre). *The Cybersecurity Act.* Dutch NCCA. Consulté le 23 avril 2024, à l'adresse https://www.dutchncca.nl/the-cybersecurityact#:~:text=The%20Cybersecurity%20Act%20(EU%20881,to%20cybersecurity%20within%20the%20EU

Moore, T. (2024, janvier). *Security Economics Knowledge Guide Issue 1.0.0.* Université de Tulsa. Consulté le 14 février 2024, à l'adresse https://www.cybok.org/media/downloads/Security_Economics_KG_v1.0.0.pdf

National Institute of Standards and Technology. (s. d.). *NIST Cybersecurity Framework*. Consulté le 17 mars 2024, à l'adresse https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

Octopus. (s. d.). *Gestion des incidents - Processus ITIL*. Consulté le 13 avril 2024, à l'adresse https://docs.octopus-itsm.com/fr/articles/gestion-des-incidents-processus-itilr

OneLogin. (2021). *Qu'est-ce que la cybersécurité et pourquoi est-elle nécessaire.* Consulté le 20 novembre 2023, à l'adresse https://www.onelogin.com/fr-fr/learn/what-is-cyber-security#:~:text=La%20cybers%C3%A9curit%C3%A9%20joue%20un%20r%C3%B4le,des%20syst%C3%A8mes%20informatiques%20d%27entreprise.

Orange Corporate. (s. d.). *Phishing : mieux comprendre et se protéger*. Consulté le 23 octobre 2023, à l'adresse https://www.orange.com/fr/engagements/orange-s-engage/pour-creer-une-societe-de-confiance/phishing-mieux-comprendre-et-se-proteger

Parlement européen. (2016). *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*. Consulté le 14 février 2024, à l'adresse https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L1148

Parlement européen et Conseil de l'Union européenne. (2022). *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).* Consulté le 20 mars 2024, à l'adresse https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022L2555

Ponemon Institute, & IBM Security. (2023). *Cost of a data breach report 2023*. IBM. Consultée le 19 février 2024, à l'adresse https://www.ibm.com/reports/data-breach

Provigis. (s. d.). *De NIS 1 à NIS 2 : l'évolution (majeure) du cadre législatif européen en matière de cybersécurité*. Consulté le 12 décembre 2023, à l'adresse https://provigis.com/blog/actualite/nis-2-evolution-cadre-legislatif-europeen

Quéméner, M. (2016). *La directive NIS, un texte majeur en matière de cybersécurité*. Sécurité et stratégie, 2016/3 (23), 50-56. Consulté le 16 décembre 2023, à l'adresse https://doi.org/10.3917/sestr.023.0050. URL: https://www.cairn.info/revue-securite-et-strategie-2016-3-page-50.htm

RedHat. (2019, 11 octobre). *La gestion des risques, qu'est-ce que c'est ?* Consulté le 16 octobre 2023, à l'adresse https://www.redhat.com/fr/topics/management/what-is-risk-management

Rédaction. (2019, 2 février). *COSO : définition*. Consulté le 8 février 2024, à l'adresse https://www.journaldunet.fr/business/dictionnaire-economique-et-financier/1198691-coso-definition/

Reuters. (2020, 12 décembre). *40 milliards d'euros, le coût de la cybercriminalité pour la Russie cette année*. Boursier. Consulté le 12 mars 2024, à l'adresse https://www.boursier.com/actualites/economie/40-milliards-d-euros-le-cout-de-la-cybercriminalite-pour-la-russie-cette-annee-45548.html

Rizzon, Y. (2022, mars 22). *La cartographie des risques : pourquoi est-ce un outil indispensable ?* SDES. Consulté le 15 ovembre 2023, à l'adresse https://sdes.fr/fiches-pratiques/la-cartographie-des-risques-pourquoi-est-ce-un-outil-indispensable/

Roy, M. M. (2022, 18 novembre). *Les technologies émergentes ont-elles un impact sur la cybersécurité ?* ManageEngine Blog. Consulté le 12 octobre 2023, à l'adresse https://blogs.manageengine.com/fr/2022/03/08/comment-les-technologies-emergentes-peuvent-avoir-un-impact-sur-la-cybersecurite.html

SafetyCulture. (2024, 15 janvier). *Gestion des risques.* Consulté le 5 février 2024, à l'adresse https://safetyculture.com/fr/themes/gestion-des-risques/

Scheelen, Y., Machilsen, K., & Deprez, A. (2023, 16 mai). *How to prepare for the NIS2 Directive ?* EY. Consulté le 6 mars 2024, à l'adresse https://www.ey.com/en_be/cybersecurity/how-to-prepare-for-the-nis2-directive

Sileyew, K. J. (2020). *Research Design and Methodology*. Dans IntechOpen eBooks. https://doi.org/10.5772/intechopen.85731

Skandrani, F. (2023, 15 mai). *Sécurité informatique et cybersécurité : quelles différences ?* IoT Industriel. Consulté le 12 novembre 2023, à l'adresse, Blog. https://iotindustriel.com/cybersecurite/securite-informatique-et-cybersecurite-quelles-differences/#:~:text=La%20cybers%C3%A9curit%C3%A9%20vise%20%C3%A0%20prot%C3%A9ger,elle%20soit%20analogique%20ou%20num%C3%A9rique.

SPF Economie. (2022, novembre 22). *Sécurité de l'information*. Consulté le 2 octobre 2023, à l'adresse https://economie.fgov.be/fr/themes/line/securite-de-linformation

Stockley, M. (2024, 9 avril). *3 important lessons from a devastating ransomware attack. Malwarebytes*. Consulté le 14 février 2024, à l'adresse https://www.malwarebytes.com/blog/ransomware/2024/03/3-important-lessons-from-a-devastating-ransomware-attack

Suganya. (2019, 24 novembre). *COBIT framework - Definition, 5 key principles & components.* ManageEngine. Consulté le 2 avril 2024, à l'adresse https://www.manageengine.com/products/service-desk/itsm/cobit-framework.html

TechTarget. (2016, 28 juillet). *Triade CIA.* LeMagIT. Consulté le 16 novembre 2023, à l'adresse https://www.lemagit.fr/definition/Triade-CIA

Terranova Security. (2022, 23 juin). *Qu'est-ce que le phishing*. Consulté le 15 octobre 2023, à l'adresse https://terranovasecurity.com/fr-fr/quest-ce-que-le-phishing/

Thompson, A. (2021, 22 avril). *What Is a DDoS Attack ?. Hashed Out By The SSL StoreTM. C*onsulté le 20 avril 2024, à l'adresse https://www.thesslstore.com/blog/what-is-a-ddos-attack/

TOPdesk. (2023, 15 décembre). *Qu'est-ce que l'ITIL Incident Management ?* TOPdesk. MCG - FR. Consulté le 27 mars 2024, à l'adresse https://www.topdesk.com/fr/glossaire/what-is-itil-incident-management/

Van Cangh, E. (2023, 21 mars). *Whitepaper : First socio-economic study on the cyber security sector in Belgium.* Agoria.
Consulté le 15 mars 2024, à l'adresse https://www.agoria.be/en/services/expertise/digitalisation/cybersecurity/whitepaper-first-socio-economic-study-on-the-cyber-security-sector-in-belgium

Van Cangh, E. (2024, 4 mai). *Business group leader*, Agoria [Entretien]. Bar à Montgomery.

Vander Geeten, V. (2024, 23 avril). *Head of legal*, CCB [Entretien]. Bureau du CCB, rue de la loi 18.

Wavestone. (2018, septembre). *De NIS 1 à NIS 2 : l'évolution (majeure) du cadre législatif européen en matière de cybersécurité*. Consulté le 14 février 2024, à l'adresse https://www.riskinsight-wavestone.com/2018/09/bilan-directive-nis/

Yves. (2023, 12 juillet). *14 types de cyberattaques les plus courants (et comment les prévenir).* Inovency. Consulté le 13 mars 2024, à l'adresse https://inovency.fr/cybersecurite/cyberattaques-types-prevenir/

Annexes

Liste des annexes :