

ECOLE NATIONALE DES SCIENCES APPLIQUÉES - KENITRA

MÉMOIRE DE PROJET DE FIN D'ÉTUDES

POUR L'OBTENTION DU DIPLÔME D'INGÉNIEUR D'ÉTAT
FILIÈRE - RÉSEAUX ET SYSTÈMES DE TÉLÉCOMMUNICATIONS (RST)

Cyber Due Diligence : Conception et mise en œuvre d'une approche et d'un Framework axés risques

Réalisé par :

BAHJA ILYAS

Encadré par :

Pr. CHOUGDALI KHALID (ENSA-K)

MME. IDRISI IMANE (DELOITTE)

M. AIT MBAREK MOHAMED AMINE
(DELOITTE)

SOUTENU LE 14 JUIN 2023 DEVANT LE JURY :

- **Pr. CHOUGDALI Khalid** : Professeur de l'enseignement supérieur, ENSA Kenitra
- **Pr. SRIFI Nabil** : Professeur de l'enseignement supérieur, ENSA Kenitra
- **Pr. RMILI Ahmed** : Professeur de l'enseignement supérieur, ENSA Kenitra

Année académique 2022/2023

ECOLE NATIONALE DES SCIENCES APPLIQUÉES - KENITRA

MÉMOIRE DE PROJET DE FIN D'ÉTUDES

POUR L'OBTENTION DU DIPLÔME D'INGÉNIEUR D'ÉTAT
FILIÈRE - RÉSEAUX ET SYSTÈMES DE TÉLÉCOMMUNICATIONS (RST)

Cyber Due Diligence : Conception et mise en œuvre d'une approche et d'un Framework axés risques

Réalisé par :

BAHJA ILYAS

Encadré par :

PR. CHOUGDALI KHALID (ENSA-K)

MME. IDRISI IMANE (DELOITTE)

M. AIT MBAREK MOHAMED AMINE
(DELOITTE)

Année académique 2022/2023

Avant-propos

Ce rapport de stage contient, par sa nature, des informations confidentielles concernant **Deloitte** et **Deloitte Morocco Cyber Center**. Il est à l'attention exclusive de son destinataire et il ne pourra donc être reproduit ou diffusé qu'avec l'accord préalable de l'entreprise.

Dédicaces

Je souhaite dédier ce rapport à ma précieuse grand-mère et à mon oncle qui ont toujours été présents pour moi. Leur soutien inconditionnel et leurs encouragements ont été d'une valeur inestimable. Je leur suis profondément reconnaissant pour tout ce qu'ils ont fait pour moi. Je tiens également à exprimer ma gratitude à ma famille et à mes amis pour leur amour et leur soutien tout au long de ce parcours.

Merci.

- Ilyas

Remerciements

Je tiens à remercier toutes les personnes qui ont contribué au succès de mon stage et qui m'ont aidé lors de la rédaction de ce rapport.

Je voudrais dans un premier temps remercier, mes tuteurs de stage : Pr. **CHOUGDALI Khalid**, Mme. **IDRISSI Imane** et M. **AIT MBAREK Mohamed Amine**, pour leur patience, leur disponibilité et surtout leurs judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je souhaite ensuite adresser mes remerciements au corps professoral et administratif de l'**École Nationale des Sciences Appliquées de KENITRA**, pour la qualité de l'enseignement offert et le soutien continu de l'équipe administrative.

Je tiens à témoigner toute ma reconnaissance aux personnes suivantes, pour leur aide et soutien dans l'élaboration de ce mémoire :

- M. **BERNOUSSI Marouane**, Senior Manager de Deloitte Morocco Cyber Center, pour m'avoir donné la chance de réaliser ce stage. Son soutien et sa bienveillance ont été d'une aide précieuse pour moi tout au long de cette expérience.
- M. **EL ASRI Reda** et M. **EL KOURTBI Mohamed**, Managers de piliers, pour m'avoir accordé leur temps et avoir répondu à mes questions. Ils ont partagé leurs connaissances et expériences dans ce milieu, tout en m'accordant leur confiance et une large indépendance dans l'exécution de missions valorisantes.
- Mme **TAZI Maha** et Mme **CHERRABI Soukaina**, Consultantes en Cybersécurité, et je voudrais les remercier pour le temps qu'elles m'ont accordé et leur aide précieuse.

Je remercie également la totalité de l'équipe de **Deloitte Morocco Cyber Center** pour leur culture de partage, leurs connaissances et leur professionnalisme, et leur support durant le déroulement de mon stage.

Acknowledgement

I would like to express my gratitude to everyone who contributed to the success of my internship and helped me throughout the writing of this report.

Firstly, I would like to thank my internship supervisors : Prof. **CHOUGDALI Khalid**, Ms. **IDRISSI Imane** and Mr. **AIT MBAREK Mohamed Amine**, for their patience, availability, and especially their valuable advice, which helped me throughout the whole internship.

I would like to extend my thanks to the faculty and administrative staff of the **National School of Applied Sciences in KENITRA** for the quality of the education provided and the continuous support of the administrative team.

I would like to express my appreciation to the following individuals for their help and support in the development of this thesis :

- Mr. **BERNOUSSI Marouane**, Senior Manager at **Deloitte Morocco Cyber Center**, for giving me the opportunity to undertake this internship. His support and kindness were invaluable to me throughout this experience.
- Mr. **EL ASRI Reda** and Mr. **EL KOURTBI Mohamed**, Pillar Managers, for giving me their time and answering my questions. They shared their knowledge and experience in this field, while granting me their trust and a large degree of independence in carrying out valuable tasks.
- Ms. **TAZI Maha** and Ms. **CHERRABI Soukaina**, Cybersecurity Consultants, I would like to thank them for the time they spent advising me and their invaluable guidance.

I would also like to thank the entire team at **Deloitte Morocco Cyber Center** for their culture of knowledge-sharing, professionalism, and support throughout my internship.

Résumé

Le présent mémoire est la synthèse d'un travail accompli dans le cadre de mon projet de fin d'études, effectué au sein de l'équipe Cyber Strategy de Deloitte Morocco Cyber Center. Il a pour objectif de réaliser la conception et la mise en œuvre d'une approche et d'un Framework de Cyber Due Diligence axés sur les risques. Ce rapport donne une vue globale sur le déroulement de stage et décrit les différentes étapes que j'ai suivies pour atteindre cet objectif, notamment la présentation de l'organisme d'accueil et du contexte général du stage, une étude théorique sur les notions de fusion et acquisition et de cybersécurité, une description détaillée de la conception de notre approche et de la réalisation de notre Framework, ainsi qu'une présentation d'une mission d'assistance en fusion et acquisition où notre approche de Cyber Due Diligence a été pleinement mise en œuvre.

Mots clés : M&A, Mergers & Acquisitions, Cyber Due Diligence, Gestion des risques Cyber, Cadre de sécurité.

Abstract

This dissertation is the culmination of work carried out as part of my end-of-study project, conducted within the Cyber Strategy team at Deloitte Morocco Cyber Center. Its objective is to design and implement a risk-driven approach and Framework for Cyber Due Diligence. This report provides an overview of the internship and describes the various steps I took to achieve this goal, including the introduction of the organization and the general context of the internship, a theoretical study on the concepts of mergers and acquisitions and cybersecurity, a detailed description of the design and implementation of our approach and Framework, and finally a presentation of an M&A assistance mission where our Cyber Due Diligence approach was fully implemented.

Keywords : M&A, Mergers & Acquisitions, Cyber Due Diligence, Cyber Risk Management, Security Framework.

Liste des abréviations

CSF	<i>Cybersecurity Framework</i>
DDoS	<i>Distributed Denial of Service</i>
DMCC	<i>Deloitte Morocco Cyber Center</i>
GSI	<i>Gestion de la Sécurité de l'Information</i>
HIPAA	<i>Health Insurance Portability and Accountability Act</i>
ICS	<i>Industrial Control System</i>
ISA	<i>International Society of Automation</i>
ISO	<i>International Organization for Standardization</i>
M&A	<i>Mergers and Acquisitions</i>
NIST	<i>National Institute of Standards and Technology</i>
OT	<i>Operational Technology</i>
OSINT	<i>Open-Source Intelligence</i>
PCI DSS	<i>Payment Card Industry Data Security Standard</i>
PCS	<i>Process Control System</i>
PHI	<i>Protected Health Information</i>
PII	<i>Personally Identifiable Information</i>
RGPD	<i>Règlement Général sur la Protection des Données</i>

SCADA *Supervisory Control and Data Acquisition*

SCF *Secure Controls Framework*

SMSI *Système de Management de la Sécurité de l'Information*

Table des figures

1.1	Chiffres d'affaires	4
1.2	Nombre d'employés	5
1.3	Positionnement du Cyber Risk Advisory	6
1.4	Deloitte Morocco Cyber Center	7
1.5	Les piliers Cyber	8
1.6	Planning du stage	13
2.1	M&A Cycle	16
2.2	Risques Cyber en M&A	22
2.3	Sections d'ISO 27001	24
2.4	Domaines de contrôles	25
2.5	NIST CSF	26
2.6	NIST 800-53 VS. ISO 27002 VS. NIST CSF	27
2.7	Frameworks entre couverture et spécialisation	31
2.8	Benchmark des normes	32
2.9	Comparaison des normes (1/2)	32
2.10	Comparaison des normes (2/2)	33
2.11	RGPD	34
2.12	HIPAA	35
2.13	PCI DSS	36
3.1	Approche globale de Cyber Due Diligence	38
3.2	Processus mis en place	39
3.3	Phase 1	40
3.4	Phase 2	41

3.5	Domaines du framewrok d'OSINT	42
3.6	Exemple des bases de données gouvernementals	44
3.7	Matrice proposée des risques	45
3.8	Consolidation des risques	46
3.9	Phase 3	47
3.10	Les domaines d'évaluation	48
3.11	Définition des niveaux d'efficacité	48
3.12	Phase 4	49
3.13	Bolt-In	50
3.14	Tuck-In	50
3.15	Consolidation	50
3.16	Transformation	51
3.17	Sous-domaines d'Information Risk Management	52
3.18	Mapping domaine 1	53
3.19	Exemples de points de contrôle du domaine 1	53
3.20	Sous-domaines de Resiliency	53
3.21	Mapping Domaine 2	54
3.22	Exemples de points de contrôle du Domaine 2	54
3.23	Sous-domaines de Operationnal Security	54
3.24	Mapping Domaine 3	56
3.25	Exemples de points de contrôle du domaine 3	56
3.26	Sous-domaines de Data Security	56
3.27	Mapping Domaine 4	57
3.28	Exemples de points de contrôle du domaine 4	57
3.29	Sous-domaines de Industry Specific Security	57
3.30	Mapping Domaine 5	58
3.31	Exemples de points de contrôles du Domaine 5	58
3.32	Sous-domaines de Leadership	58
3.33	Mapping Domaine 6	59
3.34	Exemples de points de contrôle du domaine 6	59
3.35	Sous-domaines d'Emerging Technologies	59
3.36	Mapping Domaine 7	60
3.37	Exemples de points de contrôle du domaine 7	60
3.38	Liste des feuilles visibles	60

3.39 Architecture de l'outil	61
3.40 Page d'accueil	61
3.41 Page de Scope	62
3.42 Feuille de Scope vide	62
3.43 Exemple d'automatisation des calculs	63
3.44 Workflow de la page d'accueil	64
3.45 Feuille d'OSINT Vide	65
3.46 Data Request List	65
3.47 Questionnaire préliminaire	66
3.48 Feuille des évaluations	66
3.49 Dashboard	67
4.1 Positionnement de la mission	70
4.2 Méthodologie de la mission	70
4.3 Planning prévisionnel de mission	71
4.4 Passage de la page d'accueil à la page Scope	72
4.5 Feuille de Scope (1/2)	73
4.6 Feuille de Scope (2/2)	74
4.7 Feuille d'OSINT	75
4.8 Questionnaire rempli	77
4.9 Page de risques	78
4.10 Aperçu du profil de risque de la cible	79
4.11 Aperçu du profil de risque du client	80
4.12 Risque A chez le client	81
4.13 Risque A chez la cible	81
4.14 Risque B chez le client	81
4.15 Risque B chez la cible	82
4.16 Profil consolidé	82
4.17 Risque A consolidé	83
4.18 Risque B consolidé	83
4.19 Domaines de la mission	84
4.20 Exemple de 3 contrôles de Resiliency	84
4.21 L'exemple dans la feuille	85
4.22 Feuille Dashboard	86

4.23	Graphe Radar des pourcentages d'efficacité	86
4.24	Les pourcentages d'efficacité des domaines	87
4.25	Efficacité par domaine	88
4.26	Distribution des risques	89
4.27	Distribution détaillée des risques	89
4.28	Niveau d'efficacité par niveau de risque	90

Table des matières

Avant-propos	II
Dédicaces	III
Remerciements	IV
Acknowledgement	V
Résumé	VI
Abstract	VII
Liste des abréviations	VIII
Introduction générale	1
1 Contexte général du projet	3
1 Introduction	4
2 Organisme d'accueil	4
2.1 Fiche technique de l'entreprise	4
2.2 Présentation de Risk Advisory	6
2.3 Présentation du DMCC	6
2.4 Présentation de Cyber Risk Advisory	7
2.5 Présentation du Pilier Cyber Stratégie	9
3 Cadre du projet	9
3.1 Contexte du projet	9
3.2 Problématique du projet	10

3.3	Objectifs du projet	11
3.4	Planning du stage	12
4	Conclusion	13
2	Généralités et étude de l'art	14
1	Introduction	15
2	Fusions et acquisitions (M&A)	15
2.1	Définition	15
2.2	Objectifs	15
2.3	Processus de M&A	16
2.4	Définition de la Due Diligence	17
2.5	Importance de la Due Diligence	18
3	Appui sur la cybersécurité et les risques Cyber	19
3.1	Contexte	19
3.2	Les risques Cyber	20
4	Les cadres et les normes de référence	24
4.1	ISO 27001	24
4.2	Annexe A de l'ISO 27001 et ISO 27002	25
4.3	NIST CSF	25
4.4	NIST SP 800-53	27
4.5	NIST - Guide to Operational Technology (OT) Security	28
4.6	ISA/IEC 62443	28
4.7	Cloud Controls Matrix	29
4.8	CIS Controls	29
4.9	SCF	30
4.10	Benchmark	31
5	Réglementations majeures en Cybersécurité	33
5.1	RGPD	34
5.2	HIPAA	34
5.3	PCI DSS	35
6	Conclusion	36
3	Etude fonctionnelle et conceptuelle	37
1	Introduction	38

2	Contexte	38
3	Approche globale	38
3.1	Phase 1 : Planification	39
3.2	Phase 2 : Collecte d'informations	41
3.3	Phase 3 : Réalisation des évaluations	47
3.4	Phase 4 : Rapport	49
4	Framework	51
4.1	Objectifs	51
4.2	Alimentation des contrôles de sécurité	52
4.3	Conception	60
4.4	Automatisation	62
4.5	Aperçu global	64
5	Conclusion	67
4	Mission Client	68
1	Introduction	69
2	Contexte et objectifs	69
3	Contraintes	69
4	Méthodologie	69
5	Planning prévisionnel	70
6	Application de notre approche et notre Framework	71
6.1	Planification	71
6.2	Collecte d'informations	75
6.3	Réalisation des évaluations	83
6.4	Résultats	86
7	Conclusion	91
Conclusion générale et perspectives		92
A	Annexes	94

Introduction générale

Au cours des dernières années, la croissance rapide de l'ère numérique a touché tous les secteurs de l'économie mais a aussi entraîné une augmentation des cybercrimes, des risques et des attaques informatiques. Avec l'avancement continu de la technologie, les stratégies et les capacités des acteurs malveillants cherchant à exploiter les vulnérabilités des systèmes numériques évoluent également.

Parallèlement, le marché des fusions et acquisitions connaît une période florissante où les organisations recherchent activement ces transactions afin de stimuler leur croissance et acquérir un avantage concurrentiel. Dans ce contexte, il est crucial de ne pas sous-estimer l'importance de prendre en compte les risques liés à la cybersécurité lors de ces transactions puisque ça peut entraîner des conséquences graves.

Les cybercriminels sont rapides à identifier et exploiter toute faille dans les mesures de sécurité des organisations pendant cette phase de transition où leurs défenses peuvent être temporairement affaiblies, et les conséquences d'une cyberattaque pendant cette phase peuvent être préjudiciables, entraînant des pertes financières, des dommages à la réputation, des sanctions réglementaires et même des conséquences juridiques.

Il est donc impératif pour les organisations qui s'engagent dans des activités de fusion et acquisition de donner la priorité à la gestion des risques liés à la cybersécurité tout au long du processus et de moderniser les approches adoptées.

C'est précisément dans ce contexte que s'inscrit mon projet de fin d'études, qui vise à proposer une approche moderne de Cyber Due Diligence et un Framework adéquat axés sur les risques des entités concernées lors d'une transaction en M&A.

Afin de renforcer ces propos, ce rapport présente en détail les différentes étapes que j'ai suivies pour atteindre cet objectif, qui consiste à proposer une solution efficace pour moderniser les démarches existantes de Cyber Due Diligence.

Ainsi, ce rapport est divisé en quatre chapitres. Le premier chapitre présente l'organisme d'accueil ainsi que le contexte général du stage. Le deuxième chapitre offre une étude théorique définissant les notions de fusions-acquisitions (M&A) et de cybersécurité. Par la suite, le troisième chapitre expose en détail notre démarche de conception de notre approche et la réalisation de notre Framework. Enfin, le dernier chapitre est dédié à la présentation d'une mission d'assistance en M&A à un client, où l'intégralité de notre approche de Cyber Due Diligence est mise en œuvre.

1

Contexte général du projet

1 Introduction

Ce chapitre représente une mise dans le contexte du projet, il met le point en premier lieu sur l'entreprise d'accueil, ensuite il expose la conduite du projet incluant la méthodologie de travail et la planification du stage.

2 Organisme d'accueil

Nous présentons dans ce qui suit l'organisme multinational Deloitte, sa filiale au Maroc Deloitte Morocco Cyber Center et l'équipe Cyber Stratégie qui nous a accompagné pour accomplir nos missions de stage PFE.

2.1 Fiche technique de l'entreprise

Les “Big Four” est le terme utilisé pour désigner collectivement les quatre plus grands cabinets d'audit, à savoir Deloitte, Ernst & Young, KPMG et PwC. Deloitte est réputé être le plus ancien et le plus important de ces quatre grands cabinets avec un chiffre d'affaires de 59,3 milliards de dollars (598 965 580 000,00 Dhs) pendant l'année fiscale de 2022 et environ 412 000 collaborateurs dans 150 pays. Chacun des cabinets membres constitue des entités juridiques distinctes et indépendantes entre elles.

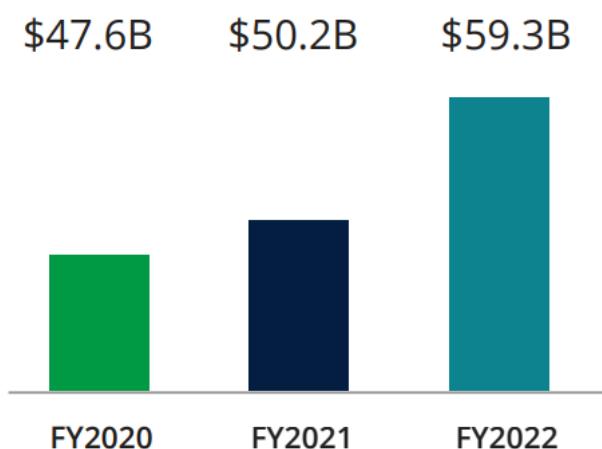


FIGURE 1.1 – Chiffres d'affaires

1. Contexte général du projet

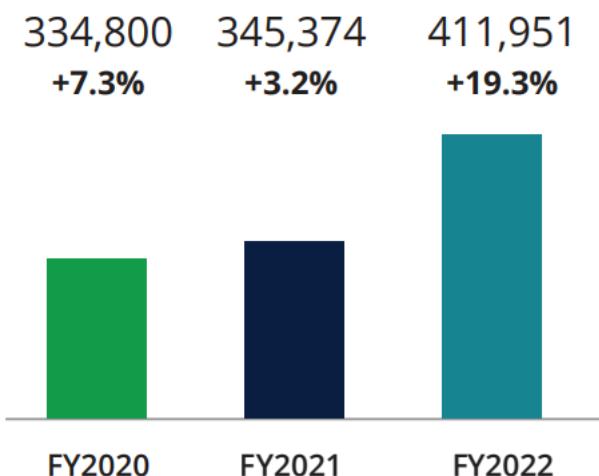


FIGURE 1.2 – Nombre d’employés

Les services offerts par le cabinet Deloitte offrent différents services selon six pôles principaux :

- **Audit et assurance** : L’audit financier consiste à donner une opinion sur l’information financière mise à la disposition des marchés financiers et des différentes parties prenantes de l’entreprise ;
- **Consulting** : De la définition de stratégies créatrices de valeur jusqu’à leur mise en œuvre concrète, les consultants aident les clients à accroître leur performance et à résoudre leurs problèmes les plus complexes ;
- **Financial Advisory** : L’audit financier consiste à donner une opinion sur l’information financière mise à la disposition des marchés financiers et des différentes parties prenantes de l’entreprise ;
- **Risk Advisory** : Les experts identifient les risques, les évaluent, les modélisent afin de prendre des décisions éclairées. Les équipes au sein du pôle Risk Advisory gèrent les différentes facettes de la gestion des risques qu’ils soient financiers, informatiques, environnementaux aux ou cyber ;
- **Tax & Legal** : Les experts proposent des solutions nouvelles qui allient à la maîtrise des problèmes juridiques et fiscaux complexes, une culture économique et financière permettant une réponse adaptée aux enjeux stratégiques des entreprises ;
- **Internal Clients Services** : Les équipes ICS accompagnent l’ensemble des métiers afin qu’ils puissent réaliser leurs missions auprès de leurs clients.

1. Contexte général du projet

2.2 Présentation de Risk Advisory

Risk Advisory s'articule autour de 5 grandes catégories de risques : risques stratégiques et de réputation, risques réglementaires, risques financiers, risques opérationnels et risques cyber.

Strategic Risk	Aider les entreprises à identifier et maîtriser les risques à fort impact sur leur stratégie en agissant sur la gouvernance, la réputation et le développement durable.
Regulatory Risk	Répondre aux demandes d'un paysage réglementaire complexe et changeant tout en restant flexible en allant jusqu'à l'externalisation.
Financial Risk	Accompagner les entreprises dans la maîtrise de leurs risques financiers et la gestion de leurs ressources rares en alliant des compétences en organisation, modélisation et processus, en s'appuyant sur des outils éprouvés.
Operational Risk	Aider les entreprises à maîtriser et piloter leurs opérations, leurs tiers, leurs données et leurs projets.
Cyber Risk	Anticiper des Cyber menaces toujours plus probables avec une approche stratégique de vigilance et de résilience.

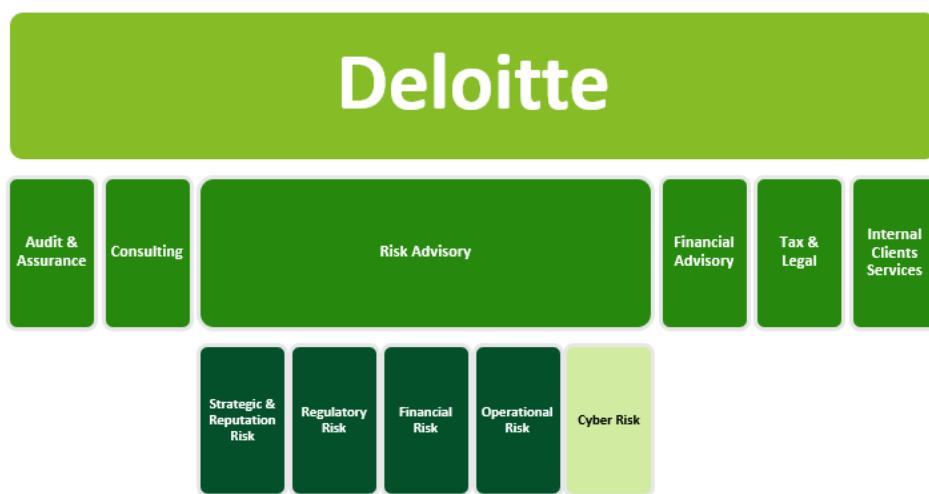


FIGURE 1.3 – Positionnement du Cyber Risk Advisory

2.3 Présentation du DMCC

Le DELOITTE MOROCCO CYBER CENTER est un centre de Cyber Intelligence qui dispose d'un pool de spécialistes cybersécurité, de technologies et de services pour répondre au besoin croissant d'expertise cyber, et pour élargir l'offre de services de Deloitte Global.

1. Contexte général du projet

Il est le premier centre cyber en Afrique à offrir des services cyber en conformité avec les meilleures pratiques en matière de cybersécurité. Le centre est situé à Casablanca, au Maroc, et fournit des services de cybersécurité aux clients dans divers secteurs d'activité, tels que les banques, les assurances, les télécommunications et les entreprises publiques. Le centre est composé d'une équipe de professionnels en cybersécurité ayant une expertise approfondie dans les domaines de la sécurité des réseaux, de la sécurité des applications et de la gestion de la sécurité d'information.



FIGURE 1.4 – Deloitte Morocco Cyber Center

2.4 Présentation de Cyber Risk Advisory

L'équipe Cyber Risk aide les organisations à mieux performer en résolvant des problèmes complexes afin de pouvoir bâtir un avenir confiant. Grâce au réseau diversifié de collaborateurs à travers le monde, Deloitte couvre tous les aspects du cyber-risque : du conseil et audit jusqu'à la mise en œuvre aux services de sécurité managés et la gestion de la réponse à incidents. Le Cyber Risk est constitué des 9 piliers Cyber suivants : L'équipe Cyber Risk aide les organisations à mieux performer en résolvant des problèmes complexes afin de pouvoir bâtir un avenir confiant. Grâce au réseau diversifié de collaborateurs à travers le monde, Deloitte couvre tous les aspects du cyber-risque : du conseil et audit jusqu'à la mise en œuvre aux services de sécurité managés et la gestion de la réponse à incidents. Le Cyber Risk est constitué des 9 piliers Cyber suivants :

1. Contexte général du projet

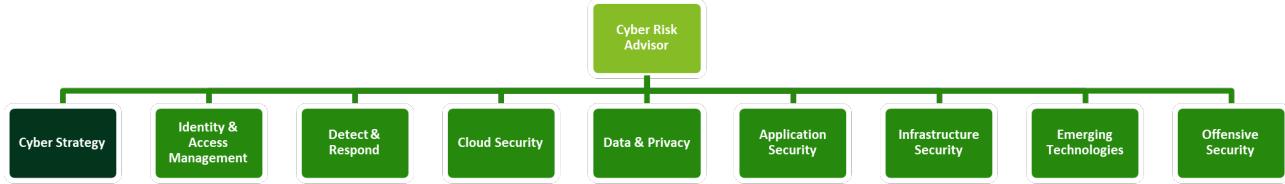


FIGURE 1.5 – Les piliers Cyber

- **Cyber Strategy** : Accompagner les clients à faire coïncider leur stratégie cyber idéale avec leurs objectifs stratégiques sur l'ensemble du périmètre de l'entreprise.
- **Identity & Access Management** : Aider les clients à assurer à la fois la sécurité des identités et des accès, et une expérience utilisateur fluide.
- **Detect & Respond** : Mettre en place des programmes de cyber défense et de gestion des incidents afin de faire face, de se protéger et de remédier aux cybers attaques.
- **Cloud Security** : Réussir la migration de tous les processus métier d'une entreprise vers le Cloud et ce de manière sécurisée et privée
- **Data & Privacy** : Aider à la gestion des informations personnelles, sensibles et confidentielles que les clients collectent, traitent et partagent.
- **Application Security** : Sécuriser les applications tout au long du cycle de développement des systèmes.
- **Infrastructure Security** : Définir les bons mécanismes afin de sécuriser le réseau et les infrastructures des organisations.
- **Emerging Technologies** : Sécuriser les technologies de nouvelle génération, telles que l'Internet des objets (IoT) et les systèmes de contrôle industriel (ICS).
- **Offensive Security** : Aider les organisations à évaluer leur résilience face aux cyberattaques en testant et examinant leurs systèmes.

2.5 Présentation du Pilier Cyber Stratégie

Les spécialistes en sécurité organisationnelle et stratégie de Deloitte aident les clients à aligner leur stratégie de cybersécurité avec leurs objectifs stratégiques dans une ère où la cybersécurité est omniprésente. L'accélération de l'innovation dans les nouvelles technologies et la génération de données rend nécessaire la réadaptation des usages, des professions et des compétences. Cette révolution numérique comporte divers avantages mais également de nombreux risques de sécurité. Deloitte aide les entreprises à aligner la stratégie de sécurité avec les priorités commerciales tout en proposant des politiques de sécurité qui apporte de la valeur à l'entreprise.

3 Cadre du projet

Dans ce qui suit, nous déclinons le contexte du projet, la problématique en question, et les objectifs qui constituent la motivation de notre projet.

3.1 Contexte du projet

De nos jours, les entreprises sont de plus en plus nombreuses à se tourner vers les fusions et acquisitions (M&A) comme moyen stratégique pour atteindre leurs objectifs de croissance. Les raisons derrière cette tendance sont multiples.

Tout d'abord, les fusions et acquisitions offrent aux entreprises une opportunité d'expansion rapide. Plutôt que de se développer organiquement sur de longues périodes, les entreprises peuvent acquérir d'autres sociétés déjà établies pour accéder à de nouveaux marchés, élargir leur portefeuille de produits ou services, ou encore renforcer leur présence géographique. Cela leur permet d'accélérer leur croissance et de gagner des parts de marché de manière plus rapide et efficace.

En outre, les fusions et acquisitions permettent aux entreprises de bénéficier de synergies. En combinant deux entités distinctes, les entreprises peuvent réaliser des économies d'échelle et améliorer leur efficacité opérationnelle en consolidant leurs infrastructures ou en partageant leurs ressources. Ces synergies peuvent se traduire par une augmentation de la rentabilité et une création de valeur pour les actionnaires.

Cependant, il convient de noter que les fusions et acquisitions comportent également des défis et des risques. Les transactions de M&A peuvent être complexes et nécessitent une planification minutieuse, une due diligence approfondie et une gestion efficace du processus d'intégration. Les

1. Contexte général du projet

entreprises doivent prendre en compte les aspects financiers, juridiques, opérationnels, culturels et cybers pour assurer le succès de la transaction.

D'ailleurs, une attention particulière doit être accordée à l'aspect cyber puisque la cybersécurité est devenue une considération critique pour les entreprises engagées dans les transactions et les processus de fusions et acquisitions en raison de son impact sur la protection des actifs numériques, la gestion des risques cyber et la préservation de la valeur de l'entreprise acquise puisque toute faille de sécurité peut entraîner des pertes financières importantes et nuire à la confiance des clients.

En négligeant la cybersécurité et en la considérant comme étant un élément secondaire dans le cadre des processus de M&A, les entreprises peuvent s'exposer à des risques importants. Les attaques informatiques peuvent non seulement entraîner des pertes financières et affecter la réputation de l'entreprise, mais peuvent aussi être liées à des problèmes de conformité réglementaire ce qui peut entraîner des conséquences à long terme.

Il est donc temps de prendre en compte le volet de la cybersécurité dans les processus de M&A afin de mieux protéger les actifs numériques, de réduire les risques liés aux cybermenaces, d'assurer une intégration plus fluide des activités post-acquisition et de garantir une transition réussie vers la nouvelle entité.

C'est dans ce cadre que s'inscrit ce projet PFE qui concerne la conception d'une approche moderne axée sur les risques de Cyber Due Diligence et l'élaboration d'un Framework et d'un outil semi-automatisé qui peut être utilisé pour offrir des services de conseil et d'accompagnement aux entreprises lors des acquisitions afin de les aider à mieux sécuriser leurs investissements.

3.2 Problématique du projet

Notre projet au sein de Deloitte aborde une problématique de sécurité globale et couvre tous les aspects critiques de la sécurité de l'entreprise. Parmi lesquels nous pouvons trouver la sécurité physique des locaux, la sécurité des données, la sécurité des réseaux et des systèmes, la sécurité des applications et des systèmes industriels, ainsi que la sécurité des fournisseurs et des partenaires externes.

En effet, lors d'une opération de M&A ou tout type d'investissement, la sécurité doit être considérée comme un élément clé pour garantir la continuité des activités, la protection des données confidentielles et la préservation de la réputation de l'entreprise.

Nous sommes conscients que les risques de sécurité sont accrus lors de ces opérations, en raison de la fusion des systèmes, des réseaux et des données de deux entités distinctes. Par

1. Contexte général du projet

conséquent, notre approche globale de la sécurité vise à garantir que les deux entités impliquées dans l'opération sont en mesure de maintenir un niveau de sécurité élevé et cohérent.

Nous sommes convaincus que la sécurité est une priorité absolue pour toute entreprise qui souhaite mener une opération d'acquisition, de fusion ou d'investissement réussi et pérenne. En prenant en compte tous les aspects de la sécurité, notre approche vise à protéger l'ensemble de l'écosystème de l'entreprise, y compris ses employés, ses clients et ses actifs, afin d'assurer la continuité des activités et de préserver la valeur de l'entreprise.

Dans un environnement numérique de plus en plus complexe et menaçant, la sécurité ne peut plus être considérée comme une question secondaire, mais plutôt comme un élément stratégique essentiel.

De nombreux clients s'appuient sur l'expertise de Deloitte pour des services d'accompagnement et de conseil dans le cadre des processus de fusion et d'acquisition, notamment dans la phase de Due Diligence où Deloitte fait face aux problèmes suivants lors des missions de conseil en matière de Cyber Due Diligence :

- **Absence d'approche standardisée et détaillée** : Les approches traditionnelles de due diligence ne suffisent plus à répondre aux besoins de sécurité numérique actuels. Le manque d'une approche moderne et détaillée de cyber due diligence peut laisser des vulnérabilités dans les systèmes, qui peuvent être exploitées par des attaquants malveillants.
- **Le besoin d'un Framework holistique** : Le besoin de concevoir un Framework bien établi pour les processus de Cyber Due Diligence.

Ces problèmes nous amènent à poser la question suivante : *Est-il possible de concevoir une approche et un cadre modernes de Cyber Due Diligence holistiques, qui couvrent tous les domaines potentiels de sécurité, tout en étant personnalisables en fonction du contexte spécifique de la transaction, et qui prennent en compte tous les risques liés aux parties prenantes concernées ?*

3.3 Objectifs du projet

A travers la problématique, nous avons constaté le besoin d'adopter une approche proactive qui couvre tous les aspects de la sécurité de l'entreprise ainsi que le besoin de concevoir un Framework bien établi et automatisé pour les processus de Cyber Due Diligence qui va en premier temps garantir un niveau élevé de sécurité en couvrant tous les domaines de sécurité nécessaires, et en deuxième temps rendre le travail des consultants plus efficace.

1. Contexte général du projet

Afin d'élaborer un cadre qui fournira un ensemble complet de directives et de contrôles de sécurité à utiliser lors des missions de Cyber Due Diligence de Deloitte, les objectifs suivants ont été fixés :

- Revue et étude des anciennes approches de Due Diligence dans le cadre des M&A et des investissements ;
- Proposition d'une approche moderne et globale de Cyber Due Diligence avec ses propres processus ;
- Analyse et étude des contrôles de sécurité et meilleures pratiques à prendre en charge des clients lors des missions de Cyber Due Diligence ;
- Elaboration d'un Framework de Cyber Due Diligence en se basant sur l'analyse précédente ;
- Conception d'un outil semi-automatisé pour rendre le Framework plus efficace.

3.4 Planning du stage

La répartition des phases du projet de ce stage, durant une période de quatre mois, est présentée selon le planning prévisionnel ci-dessous :

1. Contexte général du projet

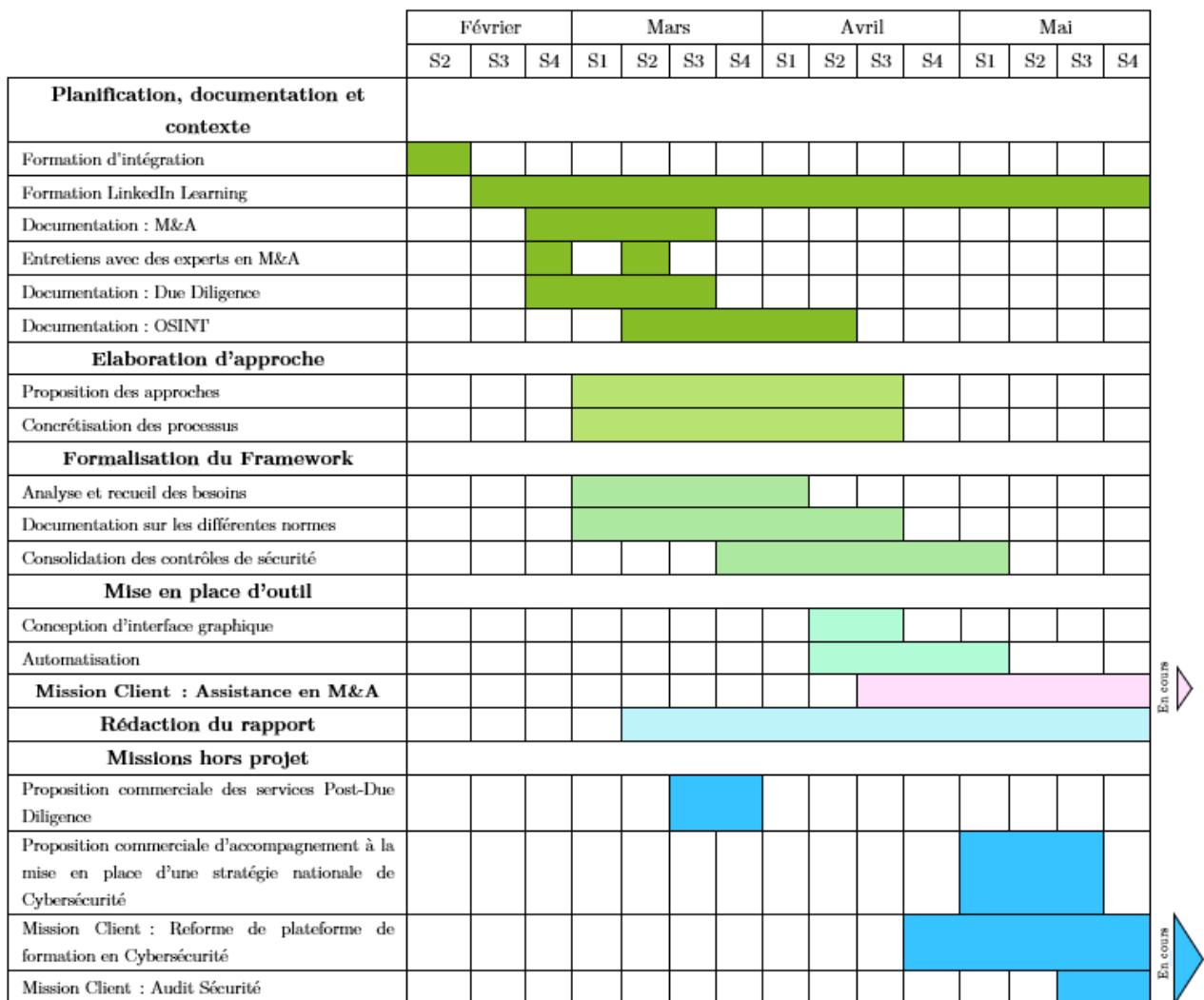


FIGURE 1.6 – Planning du stage

4 Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil et nous avons également décrit le contexte, les objectifs, la problématique et aussi le déroulement global du stage. Dans le chapitre suivant, nous aborderons la partie relative à l'état de l'art des concepts importants pour la compréhension du projet.

2

Généralités et étude de l'art

1 Introduction

Ce chapitre se focalise sur l'étude théorique des différentes technologies et concepts utiles pour la réalisation de ce projet. Dans un premier temps, nous aborderons le cycle M&A et le Due Diligence, puis nous passerons à la définition du contexte Cyber. Enfin nous discuterons les normes et les réglementations existantes en matière de sécurité et qui serviront comme input pour notre Framework.

2 Fusions et acquisitions (M&A)

2.1 Définition

Les fusions et acquisitions, ou M&A pour faire court, impliquent le processus de fusion de deux entreprises en une seule. L'objectif de la combinaison de deux ou plusieurs entreprises est de tenter d'atteindre une synergie, où l'ensemble (nouvelle entreprise) est supérieur à la somme de ses parties (les anciennes entités distinctes).

Les fusions surviennent lorsque deux entreprises s'associent. Ces transactions se produisent généralement entre deux entreprises d'environ la même taille, qui reconnaissent les avantages mutuels en termes d'augmentation des ventes, d'efficacité et de capacités. Les termes de la fusion sont souvent amicaux et convenus mutuellement, et les deux entreprises deviennent des partenaires égaux dans la nouvelle entreprise.

Les acquisitions surviennent lorsqu'une entreprise achète une autre entreprise et l'intègre à ses opérations. Parfois, l'achat est amical et parfois il est hostile, selon que l'entreprise acquise estime qu'elle est mieux en tant qu'unité opérationnelle d'une entreprise plus importante.

Le résultat final des deux processus est le même, mais la relation entre les deux entreprises diffère en fonction de la survenue d'une fusion ou d'une acquisition.

2.2 Objectifs

Les objectifs des fusions et acquisitions peuvent varier en fonction des entreprises et des situations spécifiques, mais voici quelques objectifs courants :

- **Expansion géographique** : Les entreprises peuvent chercher à étendre leur présence géographique en acquérant des entreprises dans de nouveaux marchés, régions ou pays. Cela leur permet d'accéder à de nouveaux clients, canaux de distribution et opportunités de croissance.
- **Diversification des activités** : Les entreprises peuvent chercher à diversifier leurs acti-

2. Généralités et étude de l'art

vités en acquérant des entreprises opérant dans des secteurs complémentaires. Cela réduit leur dépendance à un seul marché ou produit et permet de répartir les risques.

- **Acquisition de compétences et de technologies** : Les entreprises peuvent chercher à acquérir des compétences spécifiques, des connaissances techniques ou des technologies de pointe en fusionnant avec ou en acquérant des entreprises spécialisées. Cela renforce leur avantage concurrentiel et leur capacité d'innovation.

- **Consolidation du marché** : Les entreprises peuvent chercher à consolider leur position sur le marché en acquérant des concurrents directs ou des acteurs clés de l'industrie. Cela peut leur permettre de renforcer leur part de marché, de réduire la concurrence et d'obtenir des économies d'échelle.

- **Accès à de nouveaux clients ou segments de clientèle** : Les entreprises peuvent chercher à atteindre de nouveaux clients ou segments de clientèle en acquérant des entreprises qui ont déjà établi des relations solides avec ces marchés. Cela leur permet de gagner du temps et des efforts pour pénétrer de nouveaux marchés.

- **Rationalisation des opérations** : Les entreprises peuvent chercher à réaliser des synergies opérationnelles en fusionnant avec ou en acquérant des entreprises similaires. Cela peut inclure des économies de coûts, une consolidation des infrastructures et une meilleure utilisation des ressources.

- **Création de valeur pour les actionnaires** : Les fusions et acquisitions peuvent être entreprises dans le but de créer de la valeur pour les actionnaires en générant une croissance des revenus, une amélioration des marges, une augmentation du cours de l'action ou des dividendes plus élevés.

Ces objectifs peuvent se combiner et varier en fonction des circonstances particulières de chaque opération de fusion et acquisition. Les entreprises doivent évaluer soigneusement leurs objectifs stratégiques et les aligner sur les opportunités de marché pour maximiser les avantages potentiels de ces transactions.

2.3 Processus de M&A



FIGURE 2.1 – M&A Cycle

Le processus de fusion et acquisition comprend plusieurs étapes essentielles. Tout d'abord,

2. Généralités et étude de l'art

la stratégie M&A est développée, où l'entreprise définit ses objectifs, évalue les opportunités de marché et identifie les cibles potentielles. Cette phase implique une analyse approfondie de l'environnement commercial, y compris l'évaluation des risques et des avantages potentiels. Ensuite vient la préparation de la transaction, où les entreprises engagent des discussions préliminaires, évaluent la faisabilité financière de l'opération, négocient les termes et les conditions de la transaction, et établissent un plan d'intégration préliminaire.

Une fois que la due diligence est terminée et que les parties sont satisfaites des résultats, elles passent à la finalisation de la transaction. Cela implique la rédaction des accords définitifs, tels que les contrats d'achat, les accords de fusion ou les contrats d'investissement, et l'obtention des approbations réglementaires nécessaires. Une fois tous les documents signés et les approbations obtenues, la transaction est finalisée et la propriété de l'entreprise cible est transférée à l'acheteur.

2.4 Définition de la Due Diligence

La due diligence est une étape essentielle dans le processus de fusion-acquisition (M&A). Elle consiste en une vérification minutieuse de l'ensemble des aspects financiers, juridiques, fiscaux et opérationnels de l'entreprise cible. L'objectif est d'évaluer le potentiel de la transaction, de réduire les risques et d'identifier les opportunités.

La due diligence peut être divisée en plusieurs étapes, selon les aspects à vérifier. Tout d'abord, la due diligence financière consiste en l'analyse des états financiers et des flux de trésorerie de l'entreprise cible, afin d'identifier les éventuelles anomalies et les risques financiers. Ensuite, la due diligence juridique permet de vérifier la validité des contrats, des litiges en cours et des propriétés intellectuelles de l'entreprise cible. La due diligence fiscale permet de vérifier la conformité fiscale de l'entreprise cible et d'identifier les risques liés à la fiscalité. Enfin, la due diligence opérationnelle permet de vérifier l'efficacité des processus opérationnels de l'entreprise cible, afin d'identifier les risques opérationnels.

Les résultats de la due diligence sont utilisés pour déterminer la valeur de l'entreprise cible, négocier les modalités de la transaction et établir le plan d'intégration post-acquisition. Une due diligence bien menée peut contribuer à la réussite de la transaction, en réduisant les risques et en identifiant les opportunités.

Prenons l'exemple d'une entreprise A qui souhaite acquérir une entreprise B. Avant de finaliser la transaction, l'entreprise A doit mener une due diligence approfondie sur l'entreprise B, afin de s'assurer qu'elle est financièrement solide, qu'elle ne présente pas de risques juridiques

ou fiscaux, et qu'elle est opérationnellement efficace. Si la due diligence révèle des problèmes financiers importants ou des risques juridiques, l'entreprise A peut décider de renégocier les modalités de la transaction ou d'abandonner la transaction. Si la due diligence révèle des opportunités d'amélioration opérationnelle, l'entreprise A peut inclure ces éléments dans son plan d'intégration post-acquisition.

2.5 Importance de la Due Diligence

La due diligence en matière de fusion et acquisition revêt une importance primordiale dans le processus de transaction. Elle consiste en une analyse approfondie et diligente des aspects financiers, juridiques, opérationnels et commerciaux de l'entreprise cible. Mettre l'accent sur la due diligence lors des transactions de M&A est essentiel pour plusieurs raisons :

- **Évaluation des risques** : La due diligence permet d'identifier et d'évaluer les risques liés à l'entreprise cible. Cela inclut l'examen des aspects financiers tels que la situation comptable, les dettes, les litiges en cours, ainsi que l'analyse des aspects juridiques, réglementaires et opérationnels. L'objectif est de déterminer les risques et les défis auxquels l'acquéreur potentiel pourrait être confronté après la transaction.
- **Valorisation précise** : La due diligence permet d'évaluer de manière précise la valeur de l'entreprise cible. En examinant en détail les états financiers, les contrats, les actifs, les passifs, les flux de trésorerie et les perspectives de croissance, l'acquéreur peut déterminer le prix et les modalités de la transaction de manière éclairée.
- **Identification des opportunités** : La due diligence permet également d'identifier les opportunités de création de valeur. En analysant les synergies potentielles, les avantages concurrentiels, les synergies opérationnelles et les possibilités de croissance, l'acquéreur peut évaluer les bénéfices stratégiques et financiers que la transaction peut apporter.
- **Négociation des modalités de la transaction** : Les résultats de la due diligence fournissent une base solide pour les négociations avec l'entreprise cible. Les informations obtenues permettent de discuter des ajustements de prix, des garanties, des clauses contractuelles et d'autres éléments importants pour protéger les intérêts de l'acquéreur.
- **Préparation de l'intégration** : La due diligence fournit des informations précieuses pour la planification de l'intégration post-transaction. Elle permet d'anticiper les défis et les opportunités liés à la fusion des deux entreprises et de formuler une stratégie d'intégration solide.

La due diligence en matière de fusion et acquisition est une étape cruciale qui permet

de prendre des décisions éclairées et de minimiser les risques associés à la transaction et qui contribue à garantir le succès et la rentabilité à long terme de l'opération en évaluant les aspects financiers, juridiques, opérationnels et commerciaux de manière diligente et approfondie.

3 Appui sur la cybersécurité et les risques Cyber

3.1 Contexte

Dans le contexte actuel des affaires, la cybersécurité revêt une importance croissante en raison de nombreux facteurs qui ont contribué à en faire une préoccupation majeure pour les entreprises. Les raisons de cette préoccupation accrue sont multiples et comprennent notamment l'augmentation des cyberattaques, des violations de données et des pertes financières qui en résultent.

Tout d'abord, les cyberattaques sont devenues de plus en plus sophistiquées et fréquentes. Les hackers et les cybercriminels exploitent constamment les vulnérabilités des systèmes informatiques pour accéder à des informations sensibles, perturber les opérations commerciales et commettre des fraudes. Ces attaques peuvent prendre différentes formes, telles que les ransomwares, les attaques par phishing, les vols de données ou les intrusions malveillantes.

Ensuite, les violations de données ont également augmenté en fréquence et en ampleur. Des entreprises de toutes tailles ont été victimes de fuites de données, exposant ainsi des informations confidentielles et personnelles de leurs clients. Ces violations peuvent entraîner des conséquences graves, telles que des litiges, des amendes réglementaires, la perte de confiance des clients et des dommages à la réputation de l'entreprise.

De plus, les pertes financières associées aux cyberattaques et aux violations de données peuvent être considérables. Les coûts liés à la remédiation des attaques, à la restauration des systèmes, à la notification des clients et aux mesures de sécurité supplémentaires peuvent avoir un impact significatif sur les résultats financiers d'une entreprise. De plus, les pertes indirectes résultant d'une baisse de la confiance des clients, d'une perte de parts de marché ou de litiges peuvent également être considérables.

Enfin, les incidents de cybersécurité peuvent avoir un impact dévastateur sur la réputation d'une entreprise. La confiance des clients et des partenaires commerciaux est essentielle à la réussite d'une entreprise, et une violation de la cybersécurité peut ébranler cette confiance. Les clients sont de plus en plus exigeants en matière de protection de leurs données personnelles et de leurs informations sensibles, et les entreprises doivent démontrer leur capacité à garantir la

confidentialité et la sécurité de ces informations.

3.2 Les risques Cyber

Les risques cyber font référence aux menaces et aux vulnérabilités auxquelles les organisations sont confrontées dans le domaine de la cybersécurité. Ils englobent un large éventail de dangers liés aux activités en ligne, aux systèmes informatiques et aux données numériques.

Définition des menaces

Les menaces font référence aux dangers ou aux risques qui peuvent causer des dommages, des perturbations ou des pertes à un système, une organisation ou un individu.

Dans le contexte de la cybersécurité, les menaces sont les actions malveillantes, les activités frauduleuses ou les événements indésirables qui visent à compromettre la confidentialité, l'intégrité ou la disponibilité des données et des systèmes informatiques et peuvent provenir d'attaquants externes tels que les hackers, les cybercriminels, les groupes organisés ou d'acteurs internes malveillants tels que les employés insatisfaits ou négligents.

Définition des vulnérabilités

Les vulnérabilités font référence aux faiblesses ou aux points faibles d'un système, d'une application ou d'une infrastructure qui pourraient être exploités par des attaquants pour compromettre la sécurité. Ce sont des failles potentielles qui rendent un système plus susceptible d'être attaqué ou compromis. Les vulnérabilités peuvent résulter de problèmes de conception, de configurations incorrectes, de défauts de sécurité, de logiciels obsolètes, de pratiques, de développement insuffisantes ou d'autres erreurs humaines.

Les attaquants peuvent exploiter ces vulnérabilités pour accéder, altérer ou voler des données sensibles, perturber les opérations, exécuter des codes malveillants ou obtenir un contrôle non autorisé sur un système.

Définition des risques Cyber

Dans un monde de plus en plus connecté, où la technologie joue un rôle essentiel dans les opérations commerciales, les communications et le stockage des données, les risques cyber sont devenus un enjeu majeur. Ils englobent un large éventail de dangers liés aux activités en ligne, aux systèmes informatiques et aux données numériques. Comprendre et gérer ces risques

2. Généralités et étude de l'art

est essentiel pour prévenir les attaques malveillantes, protéger les informations sensibles et maintenir la confiance des clients.

Les risques cyber incluent les cyberattaques, qui sont des tentatives délibérées d'accéder, de perturber ou de détruire des systèmes informatiques et des réseaux. Les attaques peuvent prendre différentes formes, telles que les attaques de phishing, les logiciels malveillants, les attaques de déni de service (DDoS) et les attaques de ransomware.

Les attaquants cherchent à exploiter les vulnérabilités des systèmes pour accéder à des informations sensibles, perturber les opérations ou extorquer de l'argent. Ces attaques peuvent entraîner des pertes financières importantes, une violation de la confidentialité des informations et une perte de réputation pour les entreprises concernées.

Une autre catégorie de risques cyber concerne les violations de données, qui surviennent lorsque des informations confidentielles ou personnelles sont compromises et accessibles à des personnes non autorisées. Les violations de données peuvent résulter d'attaques cybercriminelles, de négligences internes, de vols physiques, de matériel informatique ou de défauts de sécurité.

Face à ces risques cyber, les organisations doivent mettre en place une approche globale de gestion des risques pour prévenir, détecter et atténuer les menaces.

Les risques Cyber dans les transactions de M&A

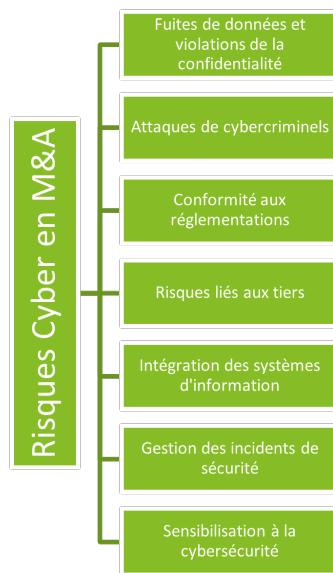


FIGURE 2.2 – Risques Cyber en M&A

Dans les transactions de fusion et acquisition (M&A), il existe des risques spécifiques en matière de cybersécurité qui doivent être pris en compte et évalués attentivement. Voici quelques-uns de ces risques :

- Fuites de données et violations de la confidentialité : L'entreprise cible peut avoir des vulnérabilités ou des lacunes dans ses mesures de sécurité qui pourraient entraîner des fuites de données sensibles ou des violations de la confidentialité des clients. Cela peut avoir un impact financier, juridique et réputationnel sur l'acquéreur potentiel.
- Attaques de cybercriminels : L'entreprise cible peut-être la cible d'attaques de cybercriminels, telles que les ransomwares, les attaques par phishing ou les intrusions malveillantes. Ces attaques peuvent compromettre les systèmes d'information, entraîner des interruptions d'activité, des pertes de données ou des vols de propriété intellectuelle.
- Conformité aux réglementations : Il est essentiel de s'assurer que l'entreprise cible respecte les réglementations en matière de cybersécurité et de confidentialité des données. Une non-conformité pourrait entraîner des sanctions financières importantes et des pertes de confiance des clients.
- Risques liés aux tiers : L'entreprise cible peut avoir des relations avec des fournisseurs, des partenaires ou des prestataires de services qui présentent des risques de sécurité importants. Il est important de comprendre ces relations et d'évaluer la sécurité des tiers impliqués pour éviter les vulnérabilités potentielles.
- Intégration des systèmes d'information : Lors de la fusion ou de l'acquisition, il est cru-

2. Généralités et étude de l'art

cial d'évaluer la compatibilité des systèmes d'information et de planifier leur intégration de manière sécurisée. Une mauvaise intégration peut créer des vulnérabilités supplémentaires et compromettre la sécurité globale des systèmes.

- **Gestion des incidents de sécurité :** Il est essentiel d'évaluer la capacité de l'entreprise cible à détecter, gérer et répondre aux incidents de sécurité. Cela inclut la mise en place de mécanismes de surveillance, de réponse aux incidents et de reprise après sinistre efficace.

- **Sensibilisation à la cybersécurité :** Les employés de l'entreprise cible doivent être conscients des meilleures pratiques en matière de cybersécurité. Une culture de la sécurité solide et des programmes de sensibilisation peuvent contribuer à réduire les risques d'attaques et de violations de données.

Il est primordial d'évaluer ces risques spécifiques en matière de cybersécurité lors des transactions de M&A afin de mettre en place des mesures appropriées de gestion des risques et de sécurité. Une due diligence approfondie dans ce domaine est essentielle pour garantir une intégration sécurisée et réussie des systèmes d'information et pour protéger les intérêts de l'acquéreur potentiel.

Impact - étude de cas

Les fusions-acquisitions peuvent avoir un impact important sur la cybersécurité des entreprises concernées. Lorsque deux entreprises se joignent, elles peuvent avoir des systèmes et des politiques de sécurité différentes, ce qui peut créer des vulnérabilités potentielles. Les entreprises doivent donc effectuer une évaluation approfondie des risques et des vulnérabilités pour s'assurer que les systèmes et les données sont protégés de manière adéquate. Par exemple, lorsque Intel a acquis McAfee en 2011, il a fallu du temps pour intégrer les deux entreprises et aligner leur approche de la sécurité.

Un autre exemple de fusion-acquisition ayant un impact sur la cybersécurité est celui de Marriott International, qui a acquis Starwood Hotels & Resorts en 2016. En 2018, il a été révélé que les données de 500 millions de clients de Starwood avaient été volées dans une violation de sécurité massive. Les enquêteurs ont déterminé que la violation avait commencé en 2014, avant que Marriott ne rachète Starwood, mais que les pirates informatiques avaient continué à accéder au réseau de Starwood pendant plusieurs années après la fusion.

4 Les cadres et les normes de référence

Dans le domaine de la cybersécurité et de la gestion des risques, il existe un certain nombre de normes et de meilleures pratiques bien établies qui aident les organisations à mettre en place des mesures efficaces de protection et de gestion des risques. Ces normes et Frameworks offrent des lignes directrices et des recommandations pour assurer la sécurité des systèmes d'information et la gestion des risques associés.

4.1 ISO 27001

ISO 27001 est une norme internationale de renom qui définit les meilleures pratiques en matière de gestion de la sécurité de l'information (GSI) au sein d'une organisation. Initialement publiée en 2005 par l'Organisation internationale de normalisation (ISO), cette norme a subi des révisions et des améliorations constantes. La version la plus récente, publiée en 2022, représente une mise à jour significative de la norme.

La norme ISO 27001 :2022 fournit un cadre complet et robuste pour la mise en place, l'implémentation, la maintenance et l'amélioration d'un système de gestion de la sécurité de l'information (SMSI) au sein d'une organisation. Elle intègre les dernières avancées technologiques, les meilleures pratiques et les nouvelles exigences en matière de sécurité de l'information.

Elle se compose de dix sections, qui définissent les exigences d'un SMSI et sont comme suit :



FIGURE 2.3 – Sections d'ISO 27001

La mise en œuvre de la norme ISO 27001 permet aux organisations de protéger leurs informations et leurs actifs contre les menaces internes et externes. Elle contribue à la mise en place

2. Généralités et étude de l'art

d'un environnement de confiance pour les partenaires commerciaux et les clients, et permet de démontrer la conformité aux exigences légales et réglementaires en matière de sécurité de l'information.

4.2 Annexe A de l'ISO 27001 et ISO 27002

L'Annexe A de la norme ISO 27001 fournit une liste détaillée des domaines de contrôle de la sécurité de l'information. Chaque domaine de contrôle fournit des lignes directrices spécifiques pour mettre en place des mesures de sécurité appropriées.

Parallèlement, l'ISO 27002 est un guide de bonnes pratiques pour la gestion de la sécurité de l'information. Il complète l'Annexe A en fournissant des directives détaillées sur la mise en œuvre des contrôles de sécurité. L'ISO 27002 aborde des aspects tels que la politique de sécurité, la gestion des actifs, la sécurité des ressources humaines, la gestion des accès, la cryptographie, la sécurité physique, la gestion des incidents, la gestion des fournisseurs, et bien d'autres encore.

En utilisant conjointement l'Annexe A et l'ISO 27002, les organisations peuvent développer un cadre solide pour évaluer, mettre en place et améliorer leur système de gestion de la sécurité de l'information. Ces documents fournissent des directives claires et pratiques qui aident les organisations à identifier les risques, à déployer les contrôles appropriés et à mettre en place des processus efficaces de gestion de la sécurité. Le graphe ci-dessous représente les domaines couverts par ces deux documents :

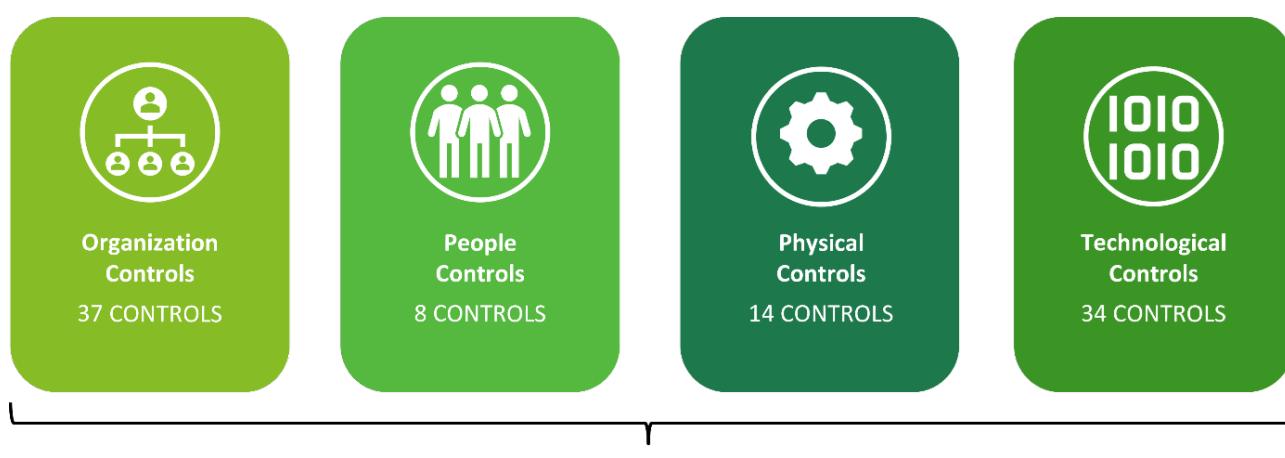


FIGURE 2.4 – Domaines de contrôles

4.3 NIST CSF



FIGURE 2.5 – NIST CSF

Le NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) est un cadre de cybersécurité développé par l’Institut national des standards et technologies (NIST) du gouvernement américain. Il fournit un ensemble de bonnes pratiques, de normes et de directives pour aider les organisations à gérer et à réduire les risques liés à la cybersécurité. Le cadre NIST CSF est devenu l’une des normes les plus largement utilisées dans l’industrie pour aider les organisations à gérer leur cybersécurité.

Le NIST CSF comprend cinq fonctions principales :

1. Identifier : Cette fonction consiste à identifier les ressources informatiques critiques, les données sensibles et les vulnérabilités afin d’évaluer les risques potentiels pour l’organisation.
2. Protéger : Cette fonction consiste à mettre en place des mesures de sécurité pour protéger les actifs critiques contre les menaces de cybersécurité.
3. Déetecter : Cette fonction consiste à surveiller les réseaux et les systèmes informatiques pour détecter les anomalies, les attaques et les intrusions.
4. Répondre : Cette fonction consiste à mettre en place des processus de réponse aux incidents de cybersécurité pour atténuer les effets des incidents, restaurer les services et minimiser les pertes.
5. Récupérer : Cette fonction consiste à mettre en place des mesures de récupération pour restaurer les données et les systèmes endommagés après un incident de cybersécurité.

Le cadre NIST CSF est conçu pour être flexible et adaptable à une grande variété d'organisations, indépendamment de leur taille, de leur secteur d'activité ou de leur maturité en matière de cybersécurité. Il fournit une structure pour les organisations qui cherchent à améliorer leur posture de cybersécurité et à gérer les risques de manière proactive. Les organisations peuvent utiliser le NIST CSF comme un cadre pour élaborer des plans d'amélioration de la cybersécurité, pour mesurer leur conformité à des normes de sécurité spécifiques et pour communiquer efficacement les enjeux de sécurité aux parties prenantes.

4.4 NIST SP 800-53



FIGURE 2.6 – NIST 800-53 VS. ISO 27002 VS. NIST CSF

Le NIST SP 800-53 (Special Publication 800-53) est un ensemble de contrôles de sécurité informatique publié par l'Institut national des normes et de la technologie (NIST) des États-Unis. Il fournit une liste de contrôles de sécurité et des recommandations pour aider les agences gouvernementales et les organisations privées à protéger leurs systèmes informatiques et leurs données.

Le document NIST SP 800-53 définit des contrôles de sécurité informatique pour les systèmes d'information fédéraux des États-Unis, mais il peut également être utilisé par d'autres organisations pour évaluer et améliorer leur posture de sécurité. Il est destiné à être utilisé comme référence pour la mise en place de mesures de sécurité de base et avancées pour les systèmes d'information.

Le document est organisé en 18 familles de contrôles de sécurité, chacune étant divisée en sous-familles. Les familles comprennent des domaines tels que la gestion de la sécurité, les contrôles d'accès, la classification et le contrôle de l'information, la sensibilisation à la sécurité et la gestion des incidents. Chaque famille de contrôle de sécurité comprend des contrôles de sécurité de base et avancés.

Les contrôles de sécurité de base sont des contrôles de sécurité minimum que toutes les organisations doivent mettre en place pour protéger leurs systèmes et leurs données. Les contrôles de sécurité avancés sont des contrôles de sécurité supplémentaires qui sont recommandés pour les organisations qui nécessitent une protection de sécurité plus forte.

4.5 NIST - Guide to Operational Technology (OT) Security

Le “Guide to Operational Technology (OT) Security” est un document publié par le National Cybersecurity Center of Excellence (NCCoE) du National Institute of Standards and Technology (NIST). Il vise à fournir des recommandations pratiques pour aider les organisations à sécuriser leurs systèmes d’exploitation, également connus sous le nom de systèmes de contrôle industriel (ICS) ou de systèmes de contrôle de processus (PCS).

Le guide commence par présenter les défis de la sécurité des systèmes d’exploitation, notamment les exigences de sécurité particulières des systèmes OT, les risques de cyber-attaques et les conséquences potentiellement catastrophiques de ces attaques sur la sécurité physique, la santé et la sécurité publique. Il fournit ensuite une description détaillée des principales catégories de menaces qui pèsent sur les systèmes OT, notamment les attaques malveillantes, les erreurs humaines et les défaillances matérielles.

Le guide fournit également une approche de sécurité pour les systèmes OT en trois étapes : la protection, la détection et la réponse. Le guide propose des recommandations spécifiques pour aider les organisations à mettre en place des contrôles de sécurité pour leurs systèmes OT, notamment des contrôles d'accès, des contrôles de sécurité réseau, des contrôles de sécurité physique et des contrôles de sécurité des systèmes.

4.6 ISA/IEC 62443

Le guide ISA/IEC 62443 est un ensemble de normes internationales pour la sécurité des systèmes de contrôle industriels (ICS) tels que les systèmes SCADA, DCS et autres systèmes de contrôle industriels. Il a été développé pour aider les organisations à protéger leurs systèmes de contrôle contre les cybermenaces qui peuvent entraîner des conséquences graves, notamment la perte de production, la pollution, les dommages matériels et les risques pour la sécurité publique.

Il propose un cadre complet pour la cybersécurité des ICS, couvrant tous les aspects de la sécurité, de la prévention à la détection, en passant par la réponse et la récupération après une cyberattaque. Il est basé sur une approche de défense en profondeur, qui implique l'utilisation

de plusieurs couches de protection pour garantir la sécurité du système et il comprend plusieurs parties, chacune couvrant un aspect spécifique de la sécurité des ICS.

Le guide ISA/IEC 62443 est largement reconnue comme l'un des cadres de cybersécurité les plus complets et les plus respectés pour les ICS. Il est utilisé par de nombreuses organisations à travers le monde pour protéger leurs systèmes de contrôle contre les cybermenaces, et il est continuellement mis à jour pour s'adapter aux nouvelles menaces et aux nouvelles technologies.

4.7 Cloud Controls Matrix

La matrice de contrôle Cloud (CCM) est un ensemble de contrôles de sécurité spécifiques à l'environnement cloud qui aide les organisations à évaluer et à gérer les risques associés à l'utilisation de services cloud. La CCM a été développée par l'association Cloud Security Alliance (CSA) et est continuellement mise à jour pour refléter les évolutions du marché des services cloud.

La matrice CCM fournit une liste détaillée de contrôles de sécurité regroupés en 17 domaines, y compris la gouvernance et la gestion des risques, les opérations et la gestion des données. Les contrôles sont conçus pour aider les organisations à évaluer la sécurité et la conformité de leur utilisation des services cloud, ainsi que pour aider les fournisseurs de services cloud à démontrer leur conformité aux normes de sécurité.

La matrice CCM est un outil important pour les organisations qui cherchent à sécuriser leurs services cloud, et pour les fournisseurs de services cloud qui cherchent à démontrer leur conformité aux normes de sécurité. En utilisant la matrice CCM, les organisations peuvent s'assurer que leurs services cloud sont sécurisés et conformes aux normes de sécurité, ce qui leur permet de réduire les risques liés à l'utilisation de services cloud et de protéger les données de l'entreprise.

4.8 CIS Controls

Le Center for Internet Security (CIS) Controls est un ensemble de bonnes pratiques de sécurité informatique qui est utilisée par de nombreuses organisations pour améliorer leur posture de sécurité. Les CIS Controls sont organisés en trois niveaux, chaque niveau contenant des sous-contrôles qui décrivent les activités que les organisations doivent mettre en place pour renforcer leur sécurité.

Les CIS Controls sont régulièrement mis à jour pour refléter les dernières menaces de sécurité et les meilleures pratiques de sécurité. Les organisations peuvent utiliser les CIS Controls pour

guider leurs activités de sécurité et s'assurer qu'elles sont conformes aux normes de sécurité de l'industrie et aux exigences réglementaires.

4.9 SCF

Le SCF (Security Control Framework) est un modèle de gestion de la sécurité des informations qui fournit une structure pour l'élaboration, la mise en œuvre et la maintenance de programmes de sécurité des informations. Il a été développé par la société de conseil en sécurité et de services de gestion de la sécurité des informations "IT Governance Ltd". Le SCF est basé sur une approche de contrôle basée sur les risques, dans laquelle les organisations peuvent évaluer leurs risques et déterminer quels contrôles de sécurité sont les plus appropriés pour atténuer ces risques.

Le SCF est divisé en cinq sections principales, chacune représentant une étape importante du processus de sécurité des informations :

- L'évaluation des risques
- La sélection des contrôles
- La mise en œuvre des contrôles
- La surveillance des contrôles
- L'amélioration continue

En utilisant le SCF, les organisations peuvent mettre en place un programme de sécurité des informations efficace qui atténue les risques associés à la sécurité des informations. Le SCF est une méthode flexible et adaptable qui peut être utilisée par les organisations de toutes tailles et dans tous les secteurs d'activité.

4.10 Benchmark

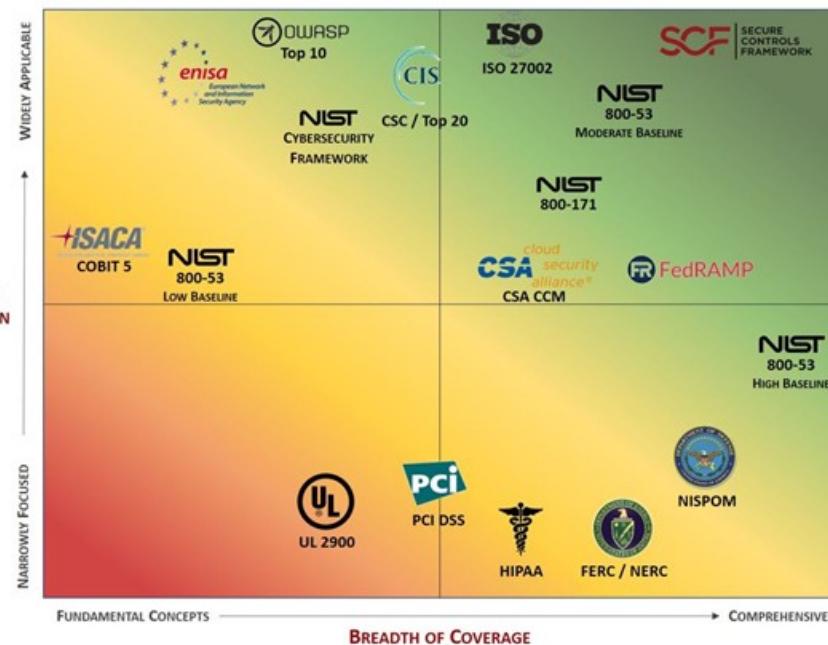


FIGURE 2.7 – Frameworks entre couverture et spécialisation

Dans le but de développer notre Framework et de le rendre largement adopté, nous avons effectué une étude approfondie et une analyse exhaustive de toutes les normes mentionnées précédemment, couvrant tous les domaines applicables et potentiels.

En se basant sur des comparaisons détaillées présentées dans des articles de recherche publiés par GARTNER et sur une étude des familles de contrôles et de caractéristiques de chaque normes et cadres mentionnés précédemment, nous avons pu conclure les résultats suivants :

2. Généralités et étude de l'art

	ISO 27001	NIST CSF	NIST SP 800- 53	NIST OT	ISA/IEC 62443	CCM	CIS	SCF
Contrôles de sécurité ciblés	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui
Contrôles de sécurité détaillés	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui
IT ou OT	IT	IT	IT	OT	OT	IT	IT	IT
Cadre de gestion des risques intégré	Non	Non	Oui	Non	Non	Non	Non	Oui
Compétences spéciales requises	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui
Scope	Global	Global	Global	OT	OT	Cloud	Global	Global
Framework personnalisable	Non	Non	Non	Non	Non	Oui	Oui	Non
Utilisation gratuite	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui

FIGURE 2.8 – Benchmark des normes

Nous avons également pu lister avantages et inconvénients clés de chacune des normes précédentes :

Normes	Avantages	Inconvénients
ISO 27001	<ul style="list-style-type: none"> Approche complète pour la gestion de la sécurité de l'information. Reconnue internationalement et largement adoptée. Établit un système de gestion de la sécurité de l'information solide. Favorise la conformité réglementaire. 	<ul style="list-style-type: none"> Peut nécessiter des ressources importantes pour la mise en œuvre et la certification. Le processus de certification peut être long et coûteux.
NIST CSF	<ul style="list-style-type: none"> Cadre de cybersécurité basé sur les risques. Large adoption et reconnaissance aux États-Unis. Flexibilité pour être adapté à différents secteurs et organisations. Met l'accent sur la gestion des risques et la résilience. 	<ul style="list-style-type: none"> Peut nécessiter une adaptation pour les organisations en dehors des États-Unis. Ne fournit pas de mesures de conformité spécifiques.
NIST SP 800-53	<ul style="list-style-type: none"> Ensemble complet de contrôles de sécurité informatique. Conçu pour les systèmes d'information fédéraux des États-Unis. Adaptabilité à différents types d'organisations. 	<ul style="list-style-type: none"> Peut être complexe et nécessiter une expertise approfondie pour l'implémentation. L'adaptation à des environnements non fédéraux peut être nécessaire.

FIGURE 2.9 – Comparaison des normes (1/2)

NIST OT	<ul style="list-style-type: none"> Fournit des directives spécifiques à la sécurité des systèmes opérationnels. S'adresse aux infrastructures critiques et aux systèmes de contrôle industriel. Alignement avec les autres publications du NIST. 	<ul style="list-style-type: none"> Peut être spécifique aux environnements industriels et nécessiter des adaptations pour d'autres secteurs. Peut être complexe et nécessiter une expertise approfondie pour l'implémentation.
ISA/IEC 62443	<ul style="list-style-type: none"> Spécifiquement conçu pour la sécurité des systèmes de contrôle industriel. Prend en compte les aspects de cybersécurité uniques aux environnements ICS. Fournit des recommandations techniques détaillées. 	<ul style="list-style-type: none"> Peut nécessiter une expertise spécialisée dans les systèmes de contrôle industriel.
CCM	<ul style="list-style-type: none"> Cadre spécifique à la sécurité du cloud. Fournit des contrôles de sécurité spécifiques aux services cloud. Facilite l'évaluation et la gestion des risques liés au cloud. 	<ul style="list-style-type: none"> Peut nécessiter des adaptations pour répondre aux besoins spécifiques d'une organisation.
CIS	<ul style="list-style-type: none"> Fournit un ensemble de bonnes pratiques en matière de sécurité informatique. Large adoption et reconnaissance. Offre des contrôles de sécurité spécifiques et pragmatiques. 	<ul style="list-style-type: none"> Peut nécessiter une adaptation pour répondre aux exigences régionales ou sectorielles spécifiques.
SCF	<ul style="list-style-type: none"> Permet de se conformer à des normes et réglementations spécifiques. Offre des contrôles de sécurité spécifiques aux exigences en vigueur. Facilite l'évaluation de la conformité. 	<ul style="list-style-type: none"> Peut être spécifique à une organisation ou une entité réglementaire particulière.

FIGURE 2.10 – Comparaison des normes (2/2)

Dans le but de développer et d'enrichir la liste des contrôles de notre Framework et le rendre exhaustive et personnalisable à la fois, nous avons pris en considération les différentes normes internationales et Frameworks discutés ainsi que certaines exigences de réglementations majeures en cybersécurité car ils se complètent mutuellement et chacun d'entre eux démontre une expertise spécifique dans un domaine précis.

5 Réglementations majeures en Cybersécurité

Les réglementations majeures en cybersécurité sont des directives et des lois qui ont été mises en place pour garantir la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques. Elles visent à assurer la protection des données personnelles des utilisateurs, à prévenir les violations de données et à promouvoir une cybersécurité efficace. Elles imposent des normes de sécurité strictes et des sanctions financières sévères en cas de non-conformité, et encouragent le partage d'informations pour lutter contre les cyberattaques.

5.1 RGPD



FIGURE 2.11 – RGPD

Le Règlement général sur la protection des données (RGPD) est une réglementation de l’Union européenne adoptée en 2016 qui est entrée en vigueur en mai 2018. Le RGPD remplace la directive européenne sur la protection des données de 1995 et a pour objectif de renforcer et d’uniformiser la protection des données personnelles au sein de l’Union européenne.

Le RGPD s’applique à toute entreprise qui traite des données personnelles de citoyens de l’Union européenne, qu’elle soit établie dans l’Union européenne ou non. Il définit les droits des individus en matière de protection des données personnelles, notamment le droit d’accès, le droit à la portabilité des données, le droit d’opposition, le droit à l’effacement et le droit à la rectification. Le RGPD oblige également les entreprises à notifier les violations de données personnelles à l’autorité de contrôle compétente et aux personnes concernées dans un délai de 72 heures après avoir eu connaissance de la violation.

Le RGPD impose des obligations de transparence et de responsabilité aux entreprises qui traitent des données personnelles, notamment en matière de conservation des données et de sécurité des données. Les entreprises doivent désigner un délégué à la protection des données (DPO) chargé de veiller à la conformité de l’entreprise avec le RGPD et de traiter les questions liées à la protection des données personnelles. En cas de non-respect du RGPD, les entreprises s’exposent à des sanctions financières pouvant atteindre 4% de leur chiffre d’affaires annuel mondial ou 20 millions d’euros, selon le montant le plus élevé.

5.2 HIPAA



FIGURE 2.12 – HIPAA

La loi sur l'assurance maladie et la responsabilité portabilité (Health Insurance Portability and Accountability Act - HIPAA) est une loi fédérale aux États-Unis qui vise à protéger les informations médicales des patients. Elle a été adoptée en 1996 et a subi plusieurs mises à jour depuis, y compris la mise en place de la règle de sécurité HIPAA en 2003. La règle de sécurité HIPAA vise à protéger la confidentialité, l'intégrité et la disponibilité des informations médicales protégées (Protected Health Information - PHI) en créant des normes de sécurité pour les organisations de santé qui traitent des informations médicales.

La règle de sécurité HIPAA est divisée en deux parties principales : la règle de sécurité des données en transit et la règle de sécurité des données stockées. La règle de sécurité des données en transit concerne la transmission de PHI, comme les transmissions par courrier électronique ou par fax, et établit des exigences pour les mesures de sécurité appropriées pour protéger ces transmissions. La règle de sécurité des données stockées concerne le stockage de PHI et établit des exigences pour les mesures de sécurité appropriées pour protéger ces données.

Les exigences de la règle de sécurité HIPAA comprennent des mesures physiques, techniques et administratives pour protéger les PHI. Les organisations de santé qui ne respectent pas les exigences de la règle de sécurité HIPAA peuvent être soumises à des sanctions civiles et pénales. Les sanctions civiles peuvent aller jusqu'à 50 000 \$ par violation et par jour, tandis que les sanctions pénales peuvent entraîner des amendes allant jusqu'à 1,5 million de dollars et une peine d'emprisonnement pouvant aller jusqu'à 10 ans.

5.3 PCI DSS



FIGURE 2.13 – PCI DSS

Le PCI DSS, ou Payment Card Industry Data Security Standard, est un ensemble de normes de sécurité des données pour les entreprises qui traitent des paiements par carte de crédit. Les entreprises qui acceptent les paiements par carte de crédit doivent se conformer aux exigences du PCI DSS afin de garantir la sécurité des données des titulaires de cartes.

Les entreprises qui ne respectent pas les exigences du PCI DSS peuvent être soumises à des amendes et à d'autres sanctions. Le PCI DSS est mis à jour régulièrement pour tenir compte des nouvelles menaces et des nouvelles technologies et les entreprises doivent rester à jour avec ses dernières exigences pour maintenir la conformité et protéger les données de leurs clients.

6 Conclusion

Dans ce chapitre, nous avons présenté les opérations d'acquisitions et de fusions et nous avons également présenté le contexte Cyber lié à ces opérations avant de décrire les normes et les réglementations existantes de Cybersécurité. Dans le chapitre suivant, nous aborderons la partie relative à l'étude fonctionnelle et conceptuelle de l'approche et le Framework réalisés.

3

Etude fonctionnelle et conceptuelle

1 Introduction

Dans ce chapitre, nous parlerons des besoins clients qui ont motivé la conception de l'approche, puis nous procéderons à la présentation de l'approche et de ses phases et processus en détails avant de présenter le Framework réalisé.

2 Contexte

Après avoir mené des entretiens avec des experts Deloitte en M&A en due diligence, il est devenu évident que les approches actuelles de la Cyber Due Diligence ne sont pas uniformisées et ne suivent pas de méthode spécifique. La plupart des approches utilisées actuellement reposent sur une liste de contrôle d'audit générique qui est ensuite adaptée au cas par cas en fonction des attentes et des besoins spécifiques du client. Bien que cette flexibilité puisse sembler avantageuse, elle présente certains inconvénients en termes d'efficacité et d'objectivité car elle peut entraîner une certaine subjectivité dans l'évaluation des risques et des vulnérabilités.

Cependant, ces constatations nous encouragent à envisager une évolution positive. Nous sommes convaincus qu'il est essentiel de développer une approche plus rigoureuse et plus structurée de la due diligence, qui permette d'assurer une analyse complète et impartiale de l'entreprise cible. En adoptant une approche plus méthodique, nous pourrons garantir une évaluation plus approfondie des risques et une compréhension plus claire des enjeux critiques.

Nous avons l'opportunité de mettre en place une approche de due diligence plus sophistiquée qui bénéficiera à toutes les parties impliquées. En suivant une méthodologie rigoureuse et transparente, nous pourrons améliorer la qualité des évaluations, accroître la confiance des parties prenantes et renforcer notre capacité à prendre des décisions éclairées.

3 Approche globale



FIGURE 3.1 – Approche globale de Cyber Due Diligence

Notre approche repose sur une méthodologie en 4 phases visant à résoudre efficacement le problème identifié et de fournir un cadre holistique et bien défini lors de la Cyber Due Diligence. En premier lieu, nous proposons une phase de planification afin d'identifier les parties prenantes

3. Etude fonctionnelle et conceptuelle

et définir les points clés et le plan de notre mission de Cyber Due Diligence ainsi qu'établir les objectifs.

Ensuite, nous passons à une phase de collecte de données et d'informations dans laquelle plusieurs processus (requête de données, OSINT, Risk profiling et un questionnaire préliminaire) sont initiés en parallèle afin d'avoir le maximum des inputs pertinents pour démarrer la troisième phase. Lors de cette dernière, nous allons effectuer une évaluation globale de la posture Cyber de l'entreprise cible, tout en se basant sur les données collectées pour personnaliser la liste des contrôles de sécurité.

Enfin, pour la dernière phase de notre approche, nous préparerons un rapport des résultats de l'évaluation ainsi qu'une élaboration des recommandations stratégiques.

Notre approche permet une optimisation des ressources en ciblant les domaines clés nécessitant une évaluation, réduisant ainsi les coûts inutiles. De plus, notre approche vise à améliorer la prise de décision en fournissant des informations précises et pertinentes aux évaluateurs et en exploitant de nombreux processus mis en place lors de chaque phase.

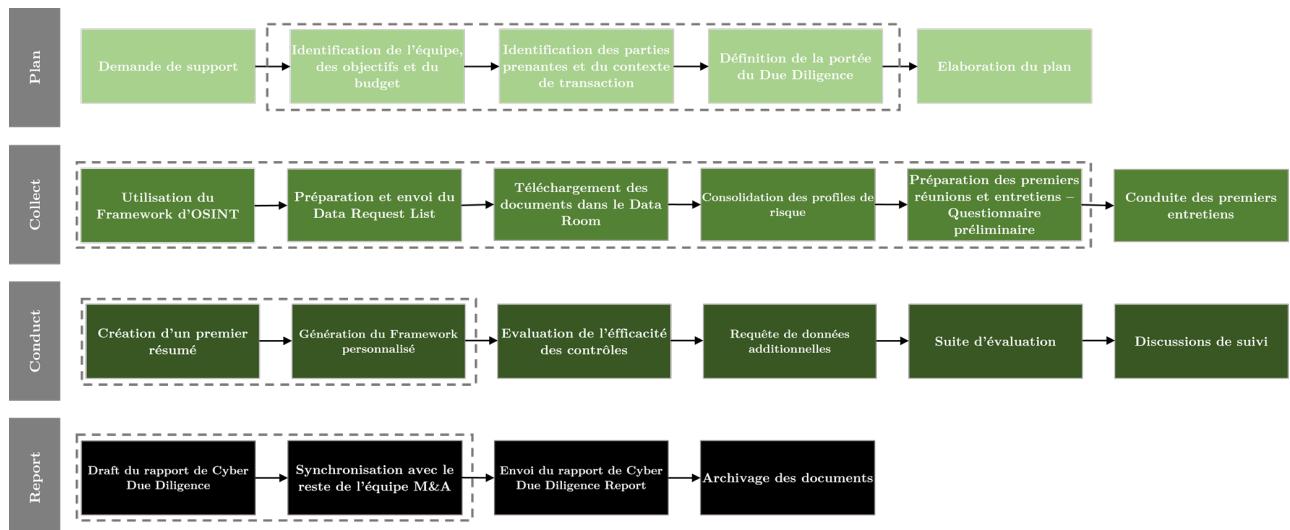


FIGURE 3.2 – Processus mis en place

3.1 Phase 1 : Planification

3. Etude fonctionnelle et conceptuelle



FIGURE 3.3 – Phase 1

La première étape du cyber due diligence est la phase de planification, qui permet d’identifier les parties prenantes clés et leurs rôles dans le processus d’évaluation de la cybersécurité. Cette phase est très importante car elle permet de définir le périmètre de l’évaluation, d’établir les objectifs et de développer un plan de projet et une ligne de temps pour l’évaluation.

Pour commencer, il est important d’identifier les parties prenantes clés dès le début de la phase de planification pour garantir leur engagement et leur participation tout au long du processus d’évaluation.

Il est aussi primordial d’identifier le contexte de transaction entre les entités concernées tout en définissant les domaines d’activités, les chiffres clés, les exigences en matière de conformité réglementaire potentielles et les normes de l’industrie auxquelles les sociétés doivent se conformer.

Cela permet de déterminer si la société cible respecte les normes de l’industrie et les réglementations applicables et nous permet aussi de pouvoir personnaliser les évaluations dans les phases qui suivent. Et puisqu’il est également important de prendre en compte les risques de cybersécurité spécifiques à l’industrie, à la géographie et aux opérations de la société cible, nous profitons de cette phase pour bien identifier ses éléments clés lors de la définition de la portée de l’évaluation tout en établissant des objectifs clairs et mesurables.

Cette phase est cruciale pour que l’évaluation soit ciblée et réponde aux besoins de la transaction. Les objectifs doivent être alignés sur les exigences réglementaires et les normes de l’industrie, ainsi que sur les risques de cybersécurité identifiés.

Une fois que le périmètre de l’évaluation et les objectifs ont été définis, il est temps de développer un plan de projet et une ligne de temps pour l’évaluation. Le plan de projet doit inclure les activités, les livrables, les rôles et les responsabilités des parties prenantes, ainsi que les délais pour chaque étape de l’évaluation. Il est également important de tenir compte des ressources nécessaires pour mener à bien l’évaluation, y compris le personnel.

3. Etude fonctionnelle et conceptuelle

En conclusion, la phase 1 du cyber due diligence est une étape cruciale pour assurer le succès de l'évaluation de la cybersécurité. Cette phase permet de définir la portée de l'évaluation, d'établir des objectifs clairs et mesurables, de développer un plan de projet et une ligne de temps pour l'évaluation, d'identifier les exigences spécifiques à l'industrie, à la géographie et aux opérations de la société cible, et d'identifier les parties prenantes clés et leurs rôles dans le Cyber Due Diligence.

3.2 Phase 2 : Collecte d'informations

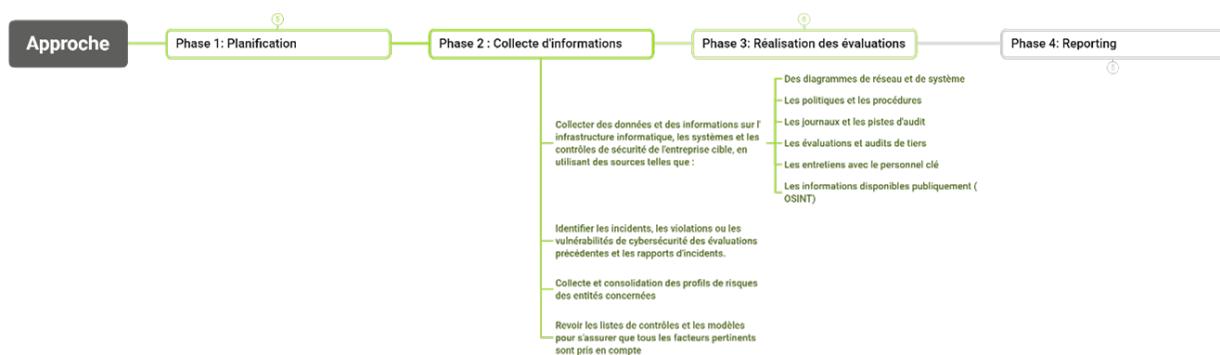


FIGURE 3.4 – Phase 2

La phase 2 du cyber due diligence est axée sur la collecte d'informations pour évaluer l'infrastructure informatique, les systèmes et les contrôles de sécurité de l'entreprise cible. Cette collecte d'informations est effectuée en parallèle à partir de différentes sources telles que les diagrammes de réseau et de système, les politiques et les procédures, les journaux et les pistes d'audit, les évaluations et les audits de tiers, les entretiens avec le personnel clé, les informations disponibles publiquement (OSINT), ainsi que les profils et matrices de risques de l'ensemble des entités concernées.

L'objectif de cette phase est d'identifier les incidents, les violations ou les vulnérabilités de cybersécurité des évaluations précédentes et les rapports d'incidents. Ces informations sont utilisées pour initialement évaluer les risques de cybersécurité et pour ensuite personnaliser la phase d'évaluation et la rendre plus pertinente.

Pour mener à bien cette phase, il est important de disposer d'une équipe compétente en matière de cybersécurité et de technologies de l'information, qui peut analyser les données et les informations collectées pour évaluer la sécurité de l'entreprise cible. Par exemple, pour la partie OSINT des consultants et des experts en Offensive Security et en Red Teaming sont ajoutés à l'équipe.

3. Etude fonctionnelle et conceptuelle

Framework d'OSINT proposé

OSINT, ou "Open Source Intelligence", est une technique d'enquête et de collecte d'informations qui consiste à utiliser des sources publiques pour obtenir des informations.

Il est largement utilisé dans les domaines de la sécurité, de l'application de la loi et de la recherche, ainsi que dans la collecte de renseignements dans le secteur privé. Les enquêteurs peuvent utiliser des outils d'OSINT pour rassembler des informations sur des suspects, des entreprises, des produits, des marques, des tendances et des événements.

L'OSINT est souvent utilisé en complément d'autres techniques d'enquête, telles que la recherche de bases de données privées, les entretiens et les enquêtes sur le terrain, ce qui est d'ailleurs notre cas puisque nous utilisons l'OSINT comme input additionnel pour nous permettre de mieux définir les éléments à évaluer. Pour cette raison, nous avons conçu un Framework d'OSINT spécifique au contexte du Cyber Due Diligence et des transactions MA.



FIGURE 3.5 – Domaines du framewrok d'OSINT

Le Framework d'OSINT que nous proposons englobe diverses sources et outils pour mener des enquêtes de renseignement en source ouverte. Il couvre à travers 11 domaines les documents publics, les bases de données gouvernementales, les dossiers judiciaires, les registres fonciers, les bases de données des organismes de réglementation, les brevets, les plateformes de médias sociaux, les forums en ligne, les sources d'actualités, le Dark Web, les moteurs de recherche, les

3. Etude fonctionnelle et conceptuelle

informations sur la structure des entreprises, les données publiques de violations et les rapports de renseignement sur les menaces, les offres d'emploi, les profils des employés, les appareils IoT et les rapports commerciaux.

Ces ressources permettent une recherche, une enquête et une analyse complètes des informations publiques afin d'obtenir des informations sur les entreprises cibles, leurs rapports commerciaux, leurs affaires juridiques, leur propriété intellectuelle ainsi que les activités sur les médias sociaux et les discussions sur les forums en ligne pour découvrir toute violation de données ou risque réputationnel entre autres, sans oublier l'exposition des appareils IoT.

En exploitant ces sources diverses, nous pouvons dresser un tableau complet et extraire des renseignements précieux qui nous aiderons à redéfinir la portée de notre évaluation.

3. Etude fonctionnelle et conceptuelle

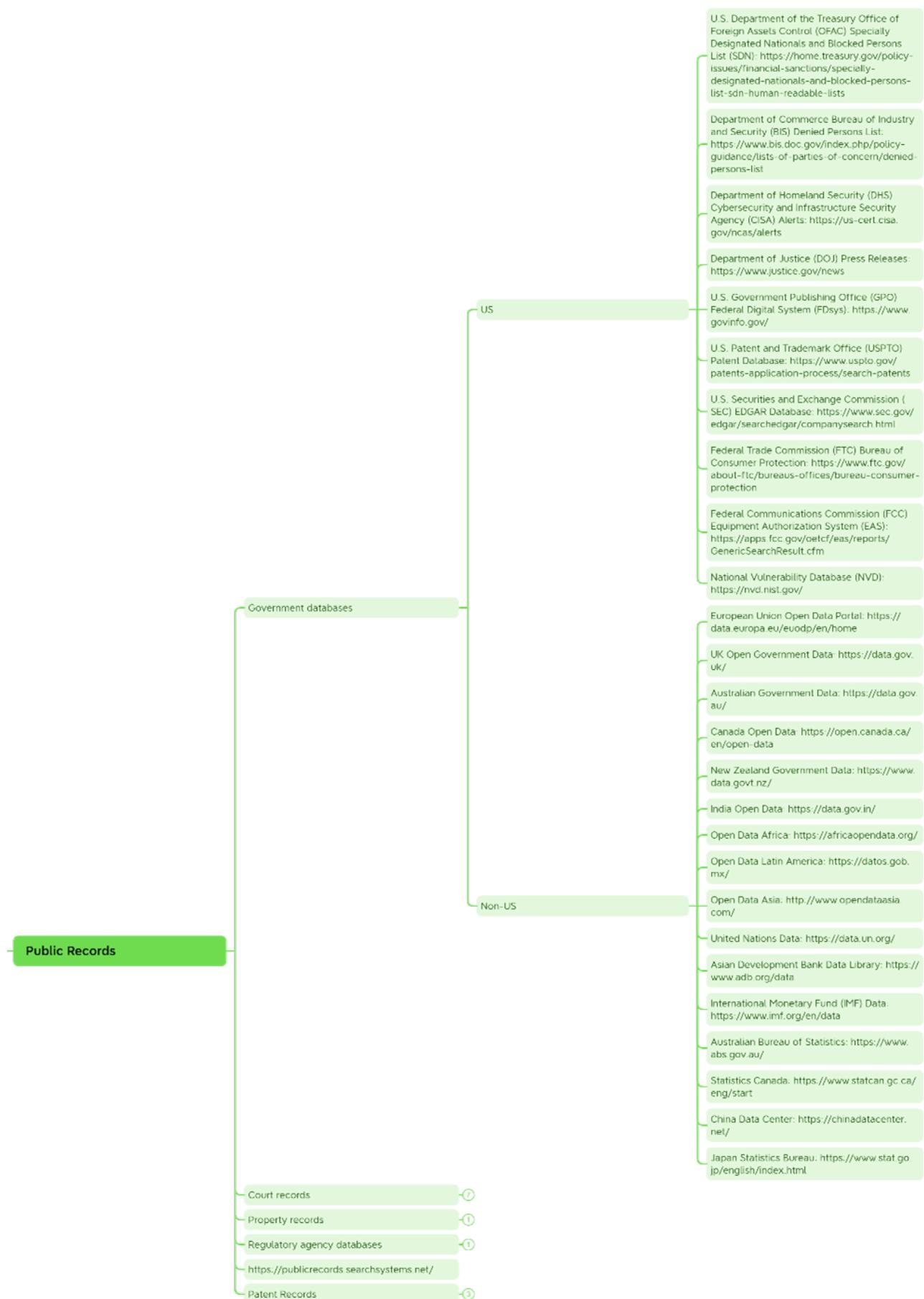


FIGURE 3.6 – Exemple des bases de données gouvernementals

3. Etude fonctionnelle et conceptuelle

Chacun des 11 domaines est constitué de plusieurs sous-domaines qui sont ensuite eux-mêmes constitués de plusieurs sources de données. La figure précédente est un exemple détaillé de l'un des sous-domaines du Framework qui couvre les outils et les sources de bases de données gouvernementales dans le contexte des entreprises américaines et non-américaines.

Elaboration du Data Request List

Dans le cadre de notre approche, l'élaboration de la liste de requêtes de données est une étape cruciale qui consiste à créer une liste complète et détaillée des informations et des données spécifiques à collecter auprès de l'entreprise cible et même auprès de l'entreprise souhaitant procéder à l'acquisition. L'objectif est de garantir une collecte exhaustive et pertinente des données nécessaires à une évaluation globale et approfondie.

L'élaboration de cette liste se fait de manière structurée, en identifiant les domaines clés d'intérêt tels que les profils de risques, l'infrastructure informatique, les systèmes, les politiques de sécurité, les processus opérationnels, le traitement des données personnelles, les contrats, etc. Chaque domaine est ensuite décomposé en sous-catégories spécifiques pour préciser les informations et les évidences requises.

Cette liste de requêtes de données joue un rôle essentiel dans la collecte d'informations pertinentes et dans la création d'une image complète de la posture de cybersécurité de l'entreprise cible. Elle permet également d'identifier les risques potentiels et les lacunes en matière de sécurité.

Collecte et consolidation des risques

		Impact				Risk Priority
		Low	Medium	High	Critical	
Likelihood	Critical	4	8	12	16	Low
	High	3	6	9	12	Medium
	Medium	2	4	6	8	High
	Low	1	2	3	4	Critical

FIGURE 3.7 – Matrice proposée des risques

La gestion des risques Cyber est définie comme un processus systématique qui vise à identifier, évaluer et traiter les risques potentiels auxquels une organisation est exposée et qui sont liés aux activités numériques, aux systèmes d'information et aux technologies utilisées.

3. Etude fonctionnelle et conceptuelle

Dans notre approche, nous proposons un processus lié directement à la gestion des risques Cyber de toutes les entités concernées. Ce processus est l'une des étapes clés de la Cyber due diligence qui consiste à collecter les profils de risque des entités concernées.

Cette collecte est réalisée en remplissant une Template bien définie qui permet de calculer automatiquement le niveau de risque en fonction d'une matrice préétablie basée sur la probabilité et l'impact où le niveau de risque égale le produit de ces deux derniers. Ce processus permet d'évaluer de manière objective les risques associés à chaque entité.

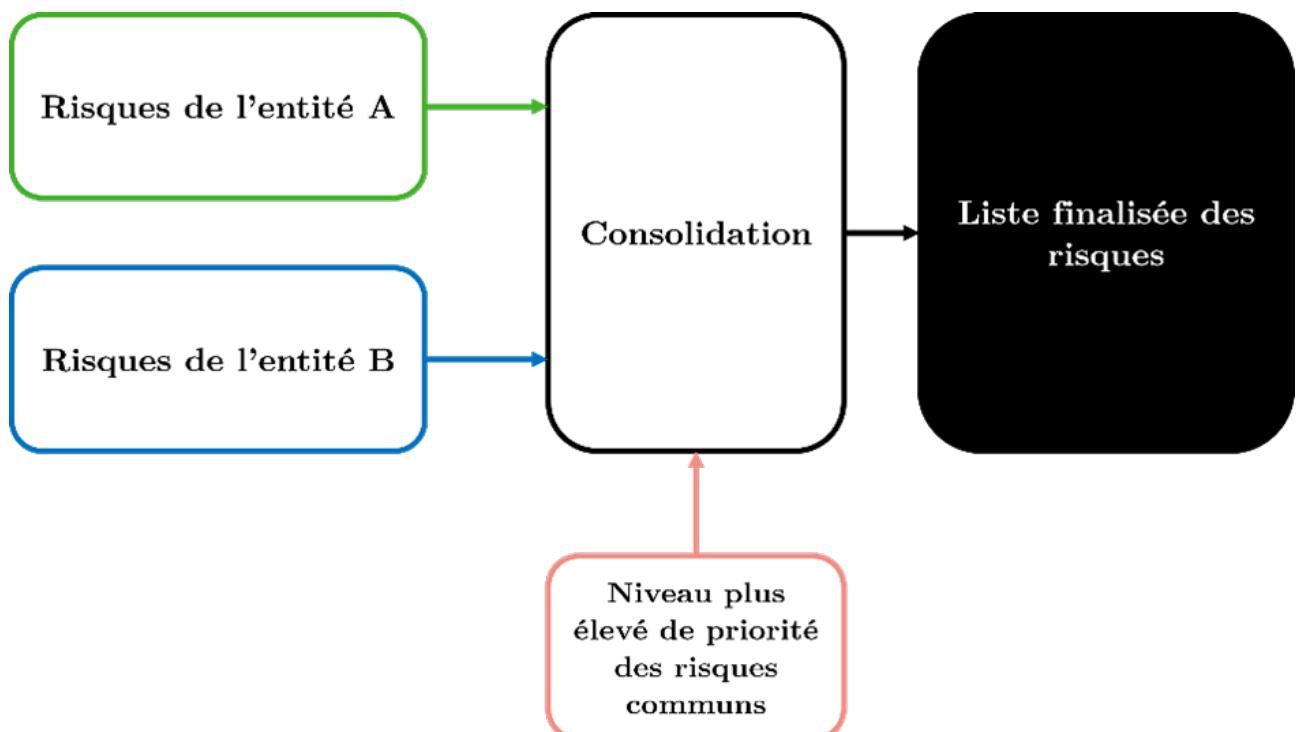


FIGURE 3.8 – Consolidation des risques

Une fois les Templates remplis, la consolidation des profils est effectuée en fusionnant les deux profils et en accordant la priorité la plus élevée aux risques communs identifiés. Ceci permet de mettre en évidence les risques les plus critiques et de se focaliser sur les points les plus sensibles pendant la phase des évaluations.

Ces processus de collecte et de consolidation des profils de risque permettent de prendre des décisions éclairées pour évaluer la posture de cybersécurité globale tout en associant une liaison directe entre les risques potentiels et les contrôles à évaluer.

Questionnaire préliminaire

Le processus de questionnaire préliminaire joue un rôle essentiel dans la personnalisation de notre Framework en permettant de recueillir des informations clés sur les activités de la société cible ainsi que sur sa posture de cybersécurité.

3. Etude fonctionnelle et conceptuelle

Le questionnaire préliminaire comprend une série de questions générales et structurées qui abordent différents aspects des activités de la société cible, de son infrastructure et de la cybersécurité, tels que la gestion des risques, la protection des données, la sensibilisation à la sécurité et les contrôles de sécurité physiques entre autres.

Les réponses fournies par la société cible permettent d'obtenir une première évaluation primitive de sa posture de cybersécurité et d'identifier les domaines à risque potentiel qui nécessitent une attention particulière lors de la phase d'évaluation approfondie. Les résultats du questionnaire orientent les prochaines étapes en personnalisant le Framework d'évaluation en mettant l'accent sur les domaines identifiés et en éliminant les domaines et les contrôles de sécurité qui sont hors contexte et hors portée.

Il est important de noter que ce questionnaire préliminaire ne constitue qu'une étape de collecte d'informations et qui est ensuite complétée par d'autres méthodes d'évaluation, telles que des entretiens et des examens documentaires. Cependant, il offre une vue d'ensemble initiale de la posture de la société cible et facilite la planification des étapes suivantes.

3.3 Phase 3 : Réalisation des évaluations

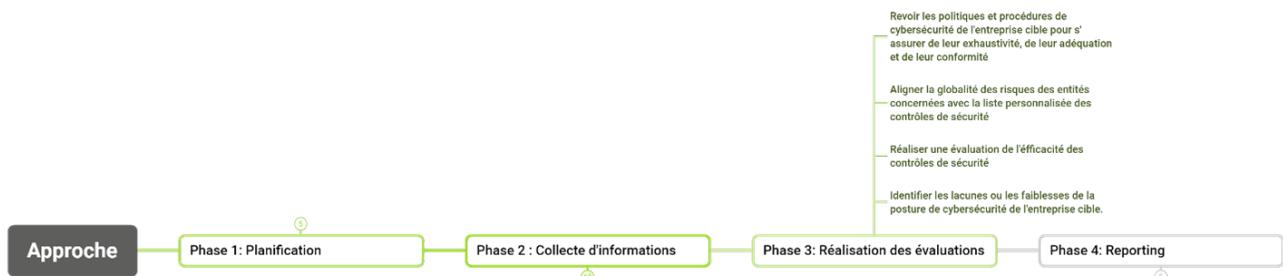


FIGURE 3.9 – Phase 3

La phase 3 du Cyber Due Diligence se concentre sur la réalisation d'évaluations de sécurité approfondies afin de mesurer l'efficacité des contrôles de sécurité de l'entreprise cible par rapport aux risques identifiés.

Ces évaluations se basent sur les outputs des phases précédentes ainsi que sur les revues de documents, les entretiens et les ateliers avec les parties prenantes, pour évaluer l'efficacité des contrôles de sécurité face aux risques identifiés.

Ces évaluations se basent sur un Framework personnalisé et automatisé, comprenant 7 domaines de sécurité qui sont subdivisés en sous-domaines, capacités, thèmes et contrôles de sécurité. Chaque évaluation est effectuée en prenant en compte trois aspects : la stratégie, la gestion et les opérations.

3. Etude fonctionnelle et conceptuelle

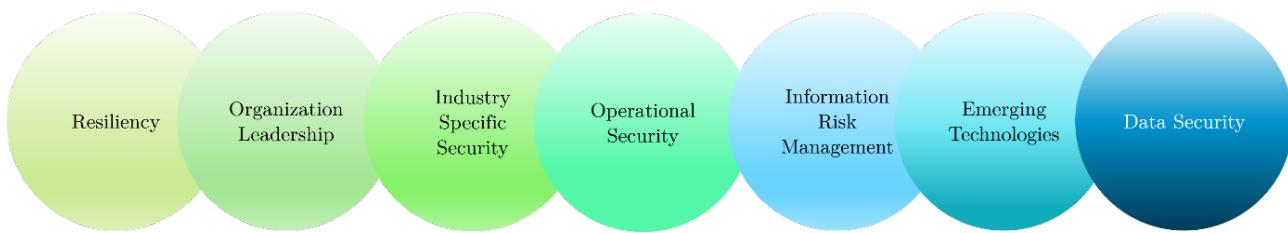


FIGURE 3.10 – Les domaines d'évaluation

La première étape consiste à associer individuellement chaque contrôle aux risques identifiés et consolidés lors de la phase précédente. Cette association permet d'attribuer automatiquement une priorité à chaque contrôle en fonction de son lien avec les risques. En répondant aux questions spécifiques à chaque contrôle, il devient possible de déterminer le niveau d'efficacité de ce contrôle par rapport au risque associé en lui attribuant un des 4 niveaux d'efficacité définis. Cette approche permet d'obtenir une évaluation précise et cohérente de chaque contrôle de sécurité.

Control Effectiveness Rating	Définition
1. Poor	Indique que des contrôles de risque efficaces n'ont pas encore été développés et qu'il existe une importante lacune en matière de contrôle des risques. Une gestion ou un traitement supplémentaire des risques est une priorité.
2. Fair/Partially Effective	Indique un besoin d'amélioration des contrôles, d'une meilleure conformité aux contrôles ou du développement de contrôles qui ne sont pas entièrement en place et testés.
3. Good	Indique une bonne gestion des risques et un système de contrôle satisfaisant, mais une possibilité de perfectionnement existe pour réduire davantage les risques.
4. Effective	Indique un risque non maîtrisé minime en raison de l'excellence des contrôles de risque en place, testés et surveillés.

FIGURE 3.11 – Définition des niveaux d'efficacité

Ce processus est répété pour l'ensemble des contrôles de sécurité, en tenant compte de la liste complète qui comprend jusqu'à 600 contrôles holistiques avant personnalisation. Chaque contrôle est minutieusement évalué en fonction de sa pertinence et de son efficacité dans la gestion des risques identifiés. Cette approche permet de créer une image complète de la robustesse des contrôles de sécurité de l'entreprise cible et de mettre en évidence les domaines où des améliorations sont nécessaires.

L'utilisation d'un Framework personnalisable et automatisé facilite le processus d'évaluation

3. Etude fonctionnelle et conceptuelle

en fournissant une méthodologie structurée et cohérente. Les évaluations réalisées dans chaque domaine de sécurité, en prenant en compte les différents aspects stratégiques, de gestion et opérationnels, permettent d'obtenir une vision globale de la posture de sécurité de l'entreprise cible et de pouvoir proposer des recommandations stratégiques dans la phase finale.

Cette approche nous permet de mesurer objectivement l'efficacité des contrôles de sécurité et d'identifier les lacunes potentielles qui nécessitent une attention particulière. De plus, l'automatisation du processus permet de gagner du temps et de garantir la cohérence des évaluations.

3.4 Phase 4 : Rapport



FIGURE 3.12 – Phase 4

La phase de rapport est la dernière phase de notre approche, permettant de consolider les résultats et de fournir des recommandations stratégiques pertinentes pour aider les clients à prendre des décisions.

Tout d'abord, un rapport sommaire est préparé, offrant un aperçu global des résultats de l'évaluation sous forme de Dashboard avec 13 graphes en total :

- Un graphe Radar affichant les pourcentages d'efficacité des contrôles de sécurité des 7 domaines ;
- Un diagramme en camembert pour visualiser la distribution des niveaux de risques dans la globalité des domaines ;
- 7 diagrammes détaillant l'efficacité des contrôles pour chaque domaine ;
- 4 diagrammes permettant de visualiser l'efficacité des contrôles par niveau de risques.

Ce rapport inclut aussi un résumé exécutif qui met en évidence les principaux points saillants, ainsi qu'un rapport technique détaillé qui fournit une analyse approfondie des conclusions pour permettre aux parties prenantes de comprendre rapidement les risques et les enjeux identifiés.

3. Etude fonctionnelle et conceptuelle

En se basant sur les résultats de l'évaluation, des recommandations et des propositions stratégiques sont élaborées pour remédier aux risques de cybersécurité détectés. Ces recommandations sont conçues de manière à être pratiques et adaptées à l'entreprise cible, prenant en compte les différentes stratégies de transformation et d'intégration qui peuvent être envisagées pour renforcer la cybersécurité de l'entreprise cible. Parmi ces stratégies, on retrouve les approches de « Transformation », « Bolt-in », « Tuck-in » et de « Consolidation ».

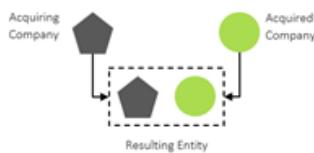


FIGURE 3.13 – Bolt-In

La stratégie « Bolt-in » consiste à intégrer de nouvelles solutions ou technologies de cybersécurité à l'infrastructure existante de l'entreprise cible. Cela peut inclure l'acquisition ou l'implémentation de logiciels, d'équipements ou de services supplémentaires visant à renforcer la protection des données et des systèmes.

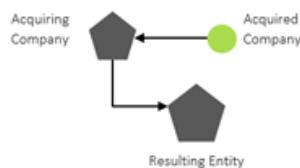


FIGURE 3.14 – Tuck-In

La stratégie « Tuck-in » implique d'intégrer complètement une entreprise spécialisée en cybersécurité à l'entreprise cible. Cela peut se faire par le biais d'une acquisition ou d'une fusion, où l'expertise et les ressources de l'entreprise spécialisée sont intégrées à la structure de l'entreprise cible.



FIGURE 3.15 – Consolidation

La stratégie de consolidation vise à rationaliser et à consolider les ressources de cybersécurité existantes au sein de l'entreprise cible. Cela peut inclure la standardisation des politiques et des procédures de sécurité, la consolidation des infrastructures technologiques ou la centralisation des équipes de cybersécurité.

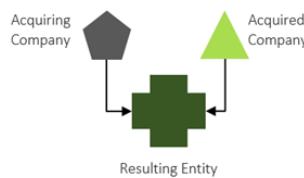


FIGURE 3.16 – Transformation

La stratégie de transformation conjointe entre l’acquéreur et l’entreprise cible (qui est généralement utilisée pour les fusions entre égaux) vise à se concentrer sur l’amélioration de la cybersécurité et à sélectionner les meilleurs processus, structures et systèmes de sécurité de chaque entreprise afin de créer une nouvelle entité dotée d’une posture de cybersécurité optimale.

Une fois les recommandations établies, elles sont ensuite priorisées en fonction de l’évaluation des risques et de l’impact potentiel sur l’entreprise cible tout en prenant en compte les domaines spécifiques où l’application de chaque stratégie peut apporter une amélioration significative de la sécurité. Les avantages potentiels de l’efficacité opérationnelle, de la réduction des coûts et de la simplification de la gestion de la cybersécurité sont aussi pris en compte.

Enfin, un suivi est réalisé avec les parties prenantes pour s’assurer que les actions recommandées sont mises en œuvre de manière appropriée. Un dialogue continu est établi pour fournir un soutien et des conseils et répondre aux questions. Ce suivi garantit que les recommandations sont effectivement mises en pratique et contribuent à améliorer la posture de cybersécurité de manière proactive et durable.

4 Framework

4.1 Objectifs

Le principal objectif de ce Framework est d’évaluer de manière structurée et cohérente la sécurité de l’entreprise cible en associant les risques aux contrôles de sécurité. Il vise également à personnaliser les contrôles de sécurité selon le contexte et automatiser les processus de l’approche du Cyber Due Diligence que nous avons proposé pour les rendre plus efficaces et optimisés.

4.2 Alimentation des contrôles de sécurité

Dans le cadre de développement du Framework, nous avons puisé notre inspiration dans plusieurs normes, cadres et réglementations reconnues. Nous avons étudié attentivement des référentiels tels que ISO 27001, plusieurs versions des cadres de NIST, les contrôles de CIS entre autres pour nous assurer que nos contrôles de sécurité sont holistiques et pertinents dans chaque domaine.

En utilisant ces références, nous nous sommes assurés que nos contrôles couvrent un large éventail de risques, tout en étant adaptés aux besoins et aux exigences spécifiques de l'entreprise cible. Nous avons cherché à établir une corrélation entre les meilleures pratiques de l'industrie et les objectifs stratégiques des entreprises, afin de garantir une approche de sécurité solide et cohérente.

Domaine 1 : Gestion des risques de l'information



FIGURE 3.17 – Sous-domaines d'Information Risk Management

Ce domaine englobe la gestion des risques liés à la cybersécurité au sein de l'organisation. Il comprend l'évaluation de la culture du risque cyber, des pratiques de gestion des risques, des politiques, des normes et de l'architecture. L'objectif est de garantir l'identification, l'évaluation et la réduction efficace des risques liés à la cybersécurité.

Il est constitué des sous-domaines suivants :

- Cyber Risk Culture and Behavior : La culture et le comportement liés à la gestion des risques cybersécuritaires au sein de l'organisation, y compris la sensibilisation des employés, la formation et les pratiques de sécurité.
- Cyber Risk Management : La gestion globale des risques cybersécuritaires, y compris l'identification, l'évaluation, la mitigation et la surveillance des risques liés aux activités de l'organisation.
- Policy, Standards and Architecture : Les politiques, les normes et les architectures de sécurité de l'information établies pour guider et soutenir la gestion des risques cybersécuritaires.

3. Etude fonctionnelle et conceptuelle

- Third Party Risk Management : La gestion des risques liés aux tiers, tels que les fournisseurs, les partenaires commerciaux et les prestataires de services, qui ont accès aux informations sensibles de l'entreprise

Nous avons alimenté le Domaine 1 par 75 points de contrôles couvrant les sous-domaines précédents tout en s'inspirant de normes et cadres spécifiques pour chaque sous-domaine, la figure suivante représente un mapping avec ces normes.



FIGURE 3.18 – Mapping domaine 1

Exemples :

Domain		Sub-Domain	Capability	Theme	Statement	Risk(s) Addressed
				Risk Appetite	Has the organization determined its cyber risk appetite? Does the organization leverage the risk appetite information for cybersecurity investments?	
					How do you ensure adherence to the established risk appetite statement?	
					Do you have a common understanding of risk appetite across the enterprise?	

FIGURE 3.19 – Exemples de points de contrôle du domaine 1

Domaine 2 : Résilience



FIGURE 3.20 – Sous-domaines de Resiliency

Le domaine de la résilience se concentre sur la capacité de l'organisation à maintenir la continuité des activités et à se rétablir après des perturbations. Il inclut l'évaluation des plans de continuité des activités, des procédures de reprise après sinistre, de la préparation aux incidents et aux crises, ainsi que des capacités de réponse aux incidents. L'objectif est de garantir que l'organisation puisse réagir de manière efficace aux incidents et rétablir ses opérations.

Il est constitué des sous-domaines suivants :

3. Etude fonctionnelle et conceptuelle

- Business Continuity Disaster Recovery : La capacité de l'organisation à maintenir ses opérations essentielles et à récupérer rapidement après un incident majeur ou une catastrophe.
- Incident and Crisis Readiness : La préparation de l'organisation pour faire face aux incidents de sécurité et aux crises, y compris la planification, les procédures et les ressources nécessaires.
- Incident Response : La capacité de l'organisation à détecter, à répondre et à gérer efficacement les incidents de sécurité informatique, y compris la collecte de preuves, l'analyse et les mesures correctives.

Le Domaine 2 a été alimenté par 70 points de contrôles mappés comme suivant :

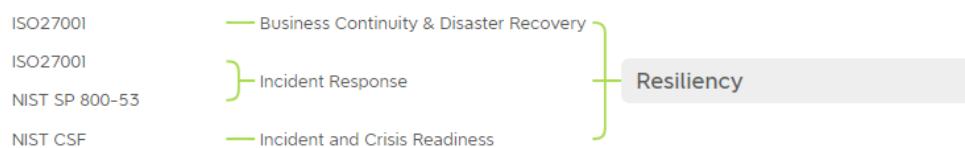


FIGURE 3.21 – Mapping Domaine 2

Exemples :

A screenshot of a Deloitte control effectiveness assessment tool. The header reads "Control Effectiveness Assessment". Below it is a table with three columns. The first column contains the standard names: ISO27001, ISO27001, NIST SP 800-53, and NIST CSF. The second column is labeled "Disaster Recovery Plan". The third column contains detailed questions for each standard. The table has a green header row and a black border.

Control Effectiveness Assessment		
ISO27001	Disaster Recovery Plan	Describe your disaster recovery strategy. Provide information on the various areas included in your disaster recovery plan that will be recovered as part of this recovery strategy.
ISO27001	Policies, Procedures and Standards	What are the procedures and strategies established to implement back-ups that align with business requirements?
NIST SP 800-53	Disaster Recovery Program	Is there a disaster recovery program in place? Describe the DRP methodology and processes.
NIST CSF		

FIGURE 3.22 – Exemples de points de contrôle du Domaine 2

Domaine 3 : Sécurité Opérationnelle



FIGURE 3.23 – Sous-domaines de Operational Security

3. Etude fonctionnelle et conceptuelle

Ce domaine couvre les aspects opérationnels de la cybersécurité. Il comprend l'évaluation des pratiques de gestion des identités et des accès, de la gestion des actifs, de la sécurité des systèmes, de la protection contre les logiciels malveillants, de la sécurité réseau, de la sécurité des appareils utilisateurs, de la sécurité des ressources humaines, de la sécurité physique, ainsi que des opérations et des communications. L'objectif est d'évaluer l'efficacité des mesures de sécurité mises en place pour protéger les opérations de l'organisation.

Il est constitué des sous-domaines suivants :

- Identity & Access Management : La gestion des identités et des accès des utilisateurs au sein du système informatique de l'organisation, y compris les autorisations, les droits d'accès et les contrôles.
- Asset Management : La gestion des actifs informatiques de l'organisation, y compris l'inventaire, la classification, la protection et la disposition appropriée des actifs.
- System Security : La sécurisation des systèmes informatiques, y compris les serveurs, les réseaux et les applications, pour prévenir les intrusions et les vulnérabilités.
- Malware Protection : La protection contre les logiciels malveillants, tels que les virus, les vers et les chevaux de Troie, pour prévenir les attaques et les infections.
- Network Security : La sécurisation du réseau informatique de l'organisation, y compris la protection contre les accès non autorisés, les attaques de déni de service et les interceptions de données.
- End-user Device Security : La sécurisation des appareils utilisés par les utilisateurs finaux, tels que les ordinateurs portables, les smartphones et les tablettes, pour prévenir les risques liés aux accès non autorisés ou à la perte de données.
- Human Resources Security : La gestion de la sécurité des ressources humaines, y compris les politiques, les procédures et les contrôles pour minimiser les risques liés aux employés.
- Physical Security : La sécurisation des locaux physiques de l'organisation, y compris les mesures de contrôle d'accès, la vidéosurveillance et la protection contre les intrusions.

Le Domaine 3 a été alimenté par 169 points de contrôles mappés comme suivant :

3. Etude fonctionnelle et conceptuelle



FIGURE 3.24 – Mapping Domaine 3

Exemples :

Control Effectiveness Assessment			
	Credential Management	Policies for Credential Management	How are password policies on setting up strong, complex passwords communicated to organizational users?
		Self Service Credential Management	What are the processes in place to perform self-service password requests?
		Event Detection and Recovery	Describe the process involved in event detection and recovery.
		Policies and Enforcement	How are Identity Management policies and standard enforced?

FIGURE 3.25 – Exemples de points de contrôle du domaine 3

Domaine 4 : Sécurité Opérationnelle



FIGURE 3.26 – Sous-domaines de Data Security

Le domaine de la sécurité des données se concentre sur la protection des informations sensibles. Il inclut l'évaluation des pratiques de confidentialité des données, de la gestion du cycle de vie des données, de la classification des informations, du chiffrement et de la prévention de la perte de données. L'objectif est de garantir que des mesures adéquates sont mises en place pour protéger la confidentialité, l'intégrité et la disponibilité des données.

Il est constitué des sous-domaines suivants :

- Data Privacy : La protection de la confidentialité et de l'intégrité des données personnelles et sensibles conformément aux réglementations sur la protection des données.
- Data Lifecycle Management : La gestion du cycle de vie des données, y compris la collecte, le stockage, l'utilisation, la transmission et la destruction sécurisée des données.

3. Etude fonctionnelle et conceptuelle

- Information Classification : La classification et l'étiquetage des informations en fonction de leur sensibilité et de leur importance, pour assurer une protection appropriée.
- Encryption : Le chiffrement des données sensibles pour prévenir l'accès non autorisé et la divulgation d'informations confidentielles.
- Data Loss Prevention : La prévention de la perte de données, y compris les mesures de prévention des fuites d'informations et de vol de données.

Le Domaine 4 a été alimenté par 76 points de contrôles mappés comme suivant :



FIGURE 3.27 – Mapping Domaine 4

Exemples :

Deloitte.		Control Effectiveness Assessment		
Data Privacy	Privacy Governance and Processes	Privacy Impact Assessments	Privacy Impact Assessments	What is the approach / process to conduct Privacy Impact Assessment (PIA) ?
		Internal and External Privacy Policy	Internal and External Privacy Policy	Do you have a repository of applicable laws and regulations for each country of operation? How is it maintained?
		Roles and Responsibilities	Privacy Request and Complaint Handling	Please describe key roles and responsibilities which are in place for data privacy.
		Privacy Request and Complaint Handling	Privacy Request and Complaint Handling	Describe processes established for privacy enquiries and complaints handling.
		Privacy Framework Management	Privacy Framework Management	Please describe any framework in place to manage data privacy.
		Compliance Management	Compliance Management	How do you identify Personally Identifiable Information (PII) database / data flows? Do you maintain a PII data inventory?

FIGURE 3.28 – Exemples de points de contrôle du domaine 4

Domaine 5 : Sécurité spécifique à l'industrie



FIGURE 3.29 – Sous-domaines de Industry Specific Security

Le domaine spécifique à l'industrie aborde les exigences spécifiques à la cybersécurité propre à l'industrie de l'organisation. Il inclut l'évaluation de la sécurité des logiciels, de la sécurité des données des détenteurs de cartes (pour l'industrie des cartes de paiement), de la sécurité des informations de santé protégées (pour le secteur de la santé), de la sécurité de la propriété

3. Etude fonctionnelle et conceptuelle

intellectuelle et d'autres considérations de sécurité propres à l'industrie. L'objectif est d'évaluer la conformité aux réglementations et normes de l'industrie.

Il est constitué des sous-domaines suivants :

- Software Security : La sécurité des logiciels développés et utilisés dans l'organisation pour prévenir les vulnérabilités et les erreurs de programmation.
- Cardholder Data Security : La sécurisation des données des titulaires de cartes de paiement conformément aux normes de sécurité des données de l'industrie des cartes de paiement.
- Protected Health Information Security : La sécurisation des informations de santé protégées conformément aux réglementations de sécurité des informations de santé.
- Intellectual Property Security : La protection de la propriété intellectuelle de l'organisation, y compris les brevets, les droits d'auteur et les secrets commerciaux.

Le Domaine 5 a été alimenté par 120 points de contrôles mappés comme suivant :

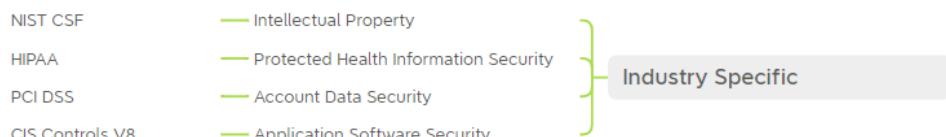


FIGURE 3.30 – Mapping Domaine 5

Exemples :

A screenshot of a Deloitte Control Effectiveness Assessment tool. The interface has a green header with the Deloitte logo. Below the header, there is a table titled "Control Effectiveness Assessment". The table has four columns. The first column contains three rows of questions related to software development security requirements, process reviews, and secure coding standards. The second column contains the corresponding answers or descriptions. The third and fourth columns are empty.

Control Effectiveness Assessment			
	Software Development Security Requirement	How are security requirements gathered and maintained?	
	SDLC Process Review and Improvements	How are security requirements integrated with the organization's regulatory tracking process? Describe the process improvement procedures	
	Secure Coding Standards, References and Procedures	How has the organization enforced secure coding practices?	

FIGURE 3.31 – Exemples de points de contrôles du Domaine 5

Domaine 6 : Leadership



FIGURE 3.32 – Sous-domaines de Leadership

Ce domaine évalue le leadership et la gouvernance de l'organisation en matière de cybersécurité. Il inclut l'évaluation de l'engagement du leadership, des structures de gouvernance, des

3. Etude fonctionnelle et conceptuelle

politiques et des mécanismes de surveillance. L'objectif est de garantir que la cybersécurité est une priorité stratégique et que des pratiques de gouvernance adéquates sont en place.

Il est constitué des sous-domaines suivants :

- Leadership Commitment : L'engagement et la responsabilité de la direction de l'organisation envers la sécurité de l'information et la gestion des risques cybernétiques.
- Governance : La gouvernance de la sécurité de l'information, y compris les structures, les politiques, les processus et les mécanismes de contrôle pour assurer une gestion efficace des risques cybernétiques.

Le Domaine 6 a été alimenté par 34 points de contrôles mappés comme suivant :



FIGURE 3.33 – Mapping Domaine 6

Exemples :

This table, titled 'Control Effectiveness Assessment' and associated with 'Deloitte', provides examples of control points for 'Organization Leadership'. It maps specific controls from three categories (KPIs, KRIs, and Contacts) to questions related to cybersecurity and privacy program management.

Control Effectiveness Assessment	
Organization Leadership	Key Performance Indicators (KPIs)
	Does the organization develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the cybersecurity and privacy program?
	Key Risk Indicators (KRIs)
	Does the organization develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the cybersecurity and privacy program?
	Contacts With Authorities
	Does the organization identify and document appropriate contacts within relevant law enforcement and regulatory bodies?

FIGURE 3.34 – Exemples de points de contrôle du domaine 6

Domaine 7 : Technologies Emergentes

- Emerging Technologies {
- Cloud Security
 - OT Security

FIGURE 3.35 – Sous-domaines d'Emerging Technologies

Le domaine des technologies émergentes concerne l'évaluation des nouvelles technologies et des tendances émergentes en matière de cybersécurité. Il inclut l'évaluation des pratiques de sécurité liées aux technologies telles que l'informatique en nuage et les technologies opérationnelles (OT). L'objectif est de comprendre les risques et les opportunités associés à ces nouvelles technologies et de s'assurer que des mesures de sécurité appropriées sont mises en place pour les exploiter de manière sécurisée.

Il est constitué des sous-domaines suivants :

3. Etude fonctionnelle et conceptuelle

- Cloud Security : La sécurité liée à l'utilisation du cloud computing dans l'organisation, y compris la protection des données, la gestion des identités et des accès, la conformité aux normes de sécurité du cloud, ainsi que la résilience et la disponibilité des services dans le cloud.
- OT Security (Operational Technology Security) : La sécurité des systèmes et des dispositifs de technologie opérationnelle utilisés dans les environnements industriels, tels que les infrastructures critiques, les systèmes de contrôle industriel (ICS) et les réseaux SCADA. Cela inclut la protection contre les cyberattaques ciblant ces systèmes, ainsi que la garantie de leur intégrité, de leur disponibilité et de leur fonctionnement sécurisé.

Le Domaine 7 a été alimenté par 43 points de contrôles mappés comme suivant :



FIGURE 3.36 – Mapping Domaine 7

Exemples :

A screenshot of a Deloitte spreadsheet titled 'Control Effectiveness Assessment'. The table has a header row 'Control Effectiveness Assessment' and several data rows under the section 'Cloud Strategy and Governance'. The data rows include:

	Control Effectiveness Assessment
Cloud Strategy	How is cloud tied into your overall security strategy and the needs of the business?
Compliance with Security Standards, Regulations and Controls Frameworks	Is an audit / compliance team in place that is responsible for conducting assessments and reviews to ensure nonconformity of established policies, procedures, and regulatory compliance obligations are addressed?
Cloud Security Service Level Agreements	Is there a process in place to conduct annual or periodic assessments to ensure compliance with contractual or regulatory compliance obligations?
	How are acceptable level of cloud services managed?

FIGURE 3.37 – Exemples de points de contrôle du domaine 7

4.3 Conception

Dans le cadre de ce projet, nous avons développé un Framework automatisé basé sur Excel avec l'utilisation de VBA (Visual Basic for Applications) et de UserForms. L'architecture de ce Framework a été conçue de manière à fournir une structure organisée et modulaire pour gérer les processus clés de notre approche de Cyber Due Diligence.

A screenshot of an Excel ribbon showing the visible sheets. The tabs are: Engagement Setup, OSINT Findings, Questionnaire, Data Request List, RiskList, Effectiveness Assessment, Dashboards, and Executive Summary. The 'Executive Summary' tab is highlighted in green.

FIGURE 3.38 – Liste des feuilles visibles

L'architecture repose sur l'identification des différents processus et la création de feuilles de calcul dédiées pour chacun d'entre eux. Nous avons 8 feuilles de calcul visible où chaque feuille est spécifiquement conçue pour stocker et gérer les informations relatives à un processus particulier, telles que la collecte par l'OSINT, la définition du périmètre, le questionnaire préliminaire et les évaluations approfondies.

3. Etude fonctionnelle et conceptuelle

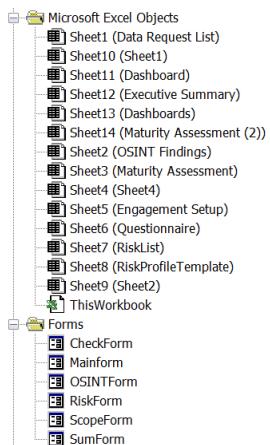


FIGURE 3.39 – Architecture de l’outil

Pour faciliter la navigation entre les processus, nous avons intégré des interfaces modernes sous forme de UserForms pour chaque processus ainsi qu’une page d’accueil qui joue le rôle d’un menu général pour pouvoir naviguer entre les processus en addition des boutons et des liens sur les feuilles de calcul. Ces éléments permettent aux utilisateurs de passer facilement d’un processus à un autre en un seul clic, offrant ainsi une expérience utilisateur fluide et intuitive.

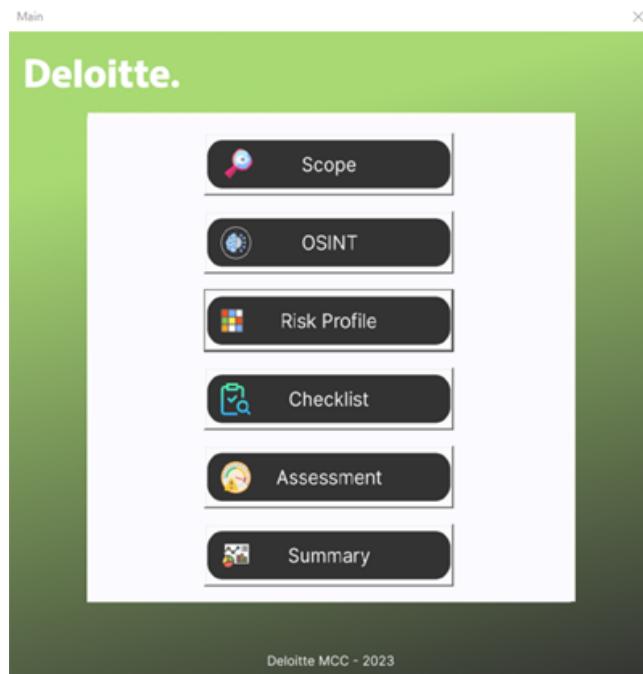


FIGURE 3.40 – Page d’accueil

Chaque page de processus est dotée par ses propres fonctionnalités permettant à l’utilisateur d’exporter les Templates de chaque processus pour les traiter et les remplir ailleurs avant de pouvoir les importer à nouveau.

3. Etude fonctionnelle et conceptuelle

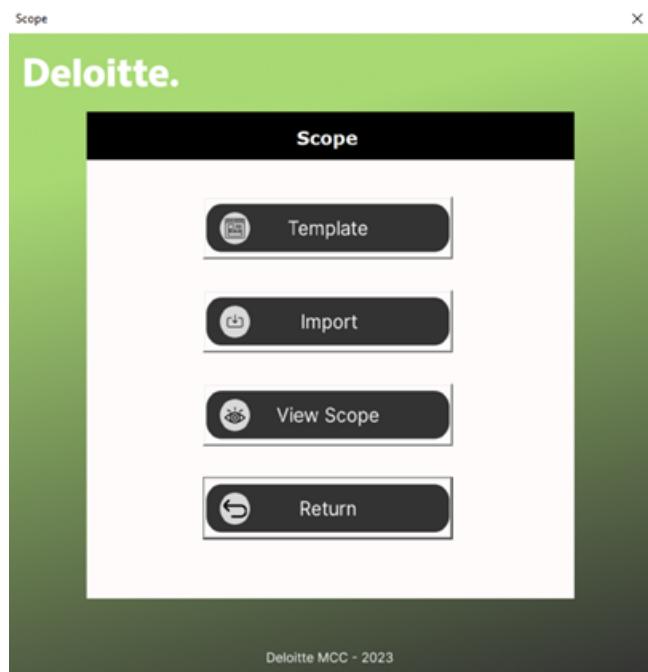


FIGURE 3.41 – Page de Scope

FIGURE 3.42 – Feuille de Scope vide

En conclusion, l'architecture utilisée pour ce Framework automatisé offre une approche pratique et efficace pour gérer les processus clés du Cyber Due Diligence. Elle permet une gestion optimisée des informations, une navigation fluide entre les processus et une expérience utilisateur améliorée.

4.4 Automatisation

L'automatisation joue un rôle essentiel dans notre Framework, nous permettant de générer des fichiers Excel individuels qui peuvent être remplis à distance avant d'être importés dans le

3. Etude fonctionnelle et conceptuelle

système.

Tout d'abord, au niveau des profils de risque, nous utilisons l'automatisation pour générer des Templates de profils de risques que nous envoyons aux parties prenantes concernées. Ces Templates incluent des champs spécifiques pour collecter les informations requises, tels que les risques, les catégories, les probabilités d'occurrence ainsi que l'impact.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Risk Name	Cause	Category	Impact	Likelihood	Risk Level	Impact								
2	TEST			High	Medium	High	Low	Medium	High	Critical					
3				#N/A			4	8	12	16					
4				#N/A			3	6	9	12					
5				#N/A			2	4	6	8					
6				#N/A			1	2	3	4					
7				#N/A											
8				#N/A											
9				#N/A											
10				#N/A											
11				#N/A											
12				#N/A											
13				#N/A											

FIGURE 3.43 – Exemple d'automatisation des calculs

L'automatisation nous permet également de calculer automatiquement les niveaux de risques en fonction des données saisies dans les templates de profils de risques. Grâce à des formules et des scripts VBA intégrés, les niveaux de risques sont déterminés de manière précise et cohérente, éliminant ainsi les erreurs humaines et les variations subjectives.

Restant toujours au niveau des profils de risque, grâce à l'automatisation lors de la consolidation de plusieurs profiles de risque, on associe automatiquement la priorité la plus haute aux risques communs.

Un autre avantage de l'automatisation est la possibilité de personnaliser les domaines et la liste de contrôles en fonction des inputs spécifiques de chaque profil de risque. En utilisant des règles et des scripts VBA, nous adaptons dynamiquement les domaines et les contrôles recommandés en fonction des caractéristiques propres à chaque profil de risque. Cela permet d'obtenir des évaluations de risques plus précises et pertinentes pour chaque contexte spécifique.

Grâce à l'automatisation, nous sommes en mesure de visualiser facilement les résultats des évaluations de risques. Nous utilisons des tableaux de bord interactifs qui récupèrent les données des fichiers Excel importés et génèrent des graphiques, des tableaux de données et des indicateurs clés de performance. Cela permet aux décideurs et aux parties prenantes de visualiser les résultats de manière conviviale et de prendre des décisions éclairées sur la base des informations présentées.

En résumé, l'automatisation de notre framework nous permet de générer des fichiers Excel individuels, de personnaliser les templates de profils de risques, de calculer automatiquement les niveaux de risques, de consolider les profils de risques et d'adapter les domaines et les contrôles, et de visualiser facilement les résultats des évaluations. Cette approche améliore

3. Etude fonctionnelle et conceptuelle

considérablement l'efficacité, la précision et la convivialité de notre système de gestion des risques, renforçant ainsi notre capacité à prendre des décisions éclairées en matière de sécurité de l'information.

4.5 Aperçu global

À travers cet aperçu, nous mettrons en avant les fonctionnalités clés et les résultats obtenus grâce à notre Framework.

Les captures d'écran ci-dessous offrent un aperçu visuel des interfaces conviviales, des tableaux de bord interactifs et des fonctionnalités d'automatisation que nous avons développés.

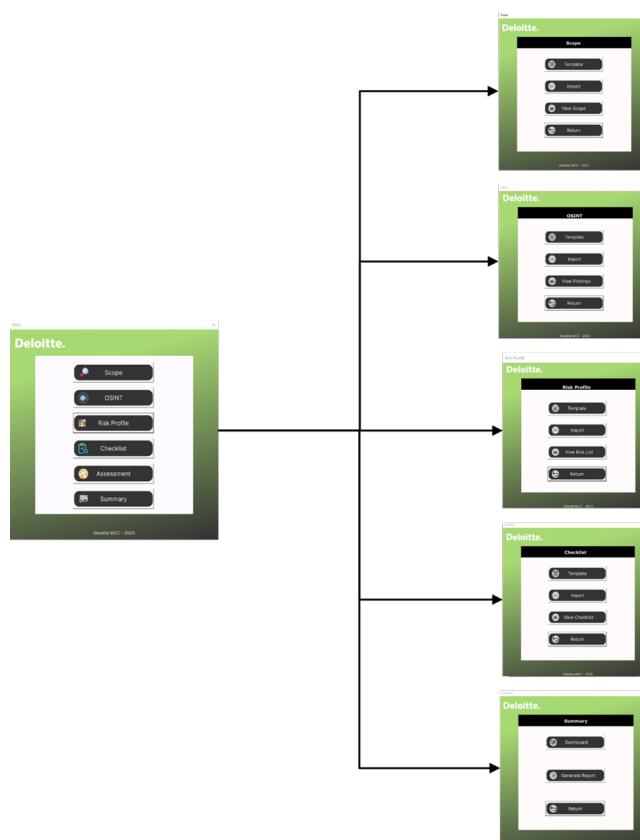


FIGURE 3.44 – Workflow de la page d'accueil

3. Etude fonctionnelle et conceptuelle

The screenshot shows a Deloitte-branded application window titled "OSINT Findings". At the top right is a "Return to Menu" button. Below the title, there are two input fields: "Date of Search:" and "Keywords Used:". A large, empty table is displayed, with the first column labeled "Source Name" and the second "Source Type". The "Source Type" column has a dropdown menu open, showing options like "Public Records", "Social Media", "Web Forums", etc., with "Public Records" currently selected. The table has columns for "ID", "Type of Information", "Findings", "Date of Finding", "Relevance", and "Additional Notes".

FIGURE 3.45 – Feuille d’OSINT Vide

The screenshot shows a Deloitte-branded application window titled "Data Request List". At the top right is a "Return to Menu" button. Below the title, there are two input fields: "Start Date:" and "Number of requests:", with the value "184" displayed. A large table is displayed, with columns for "Request ID", "Artifact", "Data Request Description", "Source", "Data Format", "Data Requested By", "Priority", "Deadline", "Status", and "Notes". The table contains several entries, such as RP-1 (Risk Profile of Target), RP-2 (Risk Profile of Client), and various entries under E-GOV-01 through E-GOV-07, each with a different artifact type and description.

FIGURE 3.46 – Data Request List

3. Etude fonctionnelle et conceptuelle

Deloitte.

Initial Questionnaire

 [Return to Menu](#)

Question #	Question	Question type	Answer	Notes
1	What type of business does your organization conduct?	Open Question		
2	How many employees does your organization have?	Open Question		
3	What is the size of your organization's IT infrastructure?	Open Question		
4	Does your organization use any industrial control systems (ICS) or supervisory control and data acquisition (SCADA) systems in your operations?	Yes/No		
5	Is there a cybersecurity department within the organization?	Yes/No		
6	Does your organization outsource any security functions to third-party service providers?	Yes/No		
7	Has your organization ever experienced a significant cybersecurity incident?	Yes/No		
8	Does your organization maintain an inventory of all hardware and software assets?	Yes/No		
9	Does your organization have a formal security policy in place?	Yes/No		
10	What types of cybersecurity policies do you have in place in your organization today?	Open Question		
11	Does your organization use cloud services?	Yes/No		
12	Does your organization develop custom software applications?	Yes/No		
13	Does your organization have a process in place for managing software patches and updates?	Yes/No		
14	Does your organization process or store sensitive information?	Yes/No		
15	What type of sensitive information does your organization process or store?	Multiple Choice		
16	Does your organization have a disaster recovery plan?	Yes/No		
17	Does your organization have an incident response plan?	Yes/No		

FIGURE 3.47 – Questionnaire préliminaire

Deloitte.

Control Effectiveness Assessment

Domain	Sub-Domain	Capability	Theme	Statement	Point(s) Addressed	Risk Priority	Answer	Control Effectiveness Rating	Evidence	Notes
Cyber risk culture and behavior	Risk Culture	Risk Appetite	Who is responsible for promoting the cyber security vision and culture?	Has the organization developed its cyber security appetite? Does the organization leverage the risk appetite information for cybersecurity investments?	None	Medium				
			What role does it play in managing cyber risk?	How do you ensure adherence to the established risk appetite in management?	None	Medium				
		Cyber Risk Culture	What role does it play in managing cyber risk?	Who is responsible for promoting the cyber security vision and culture?	None	Medium				
			What role does it play in managing cyber risk?	What role does it play in managing cyber risk?	None	Medium				
	Cyber Risk Discussions at Board Level	Cyber Risk Discussions at Board Level	What is the general level of buy-in from the board and stakeholders toward cyber risk?	What is the general level of buy-in from the board and stakeholders toward cyber risk?	None	Medium				
		Cyber Communications	Who communicates on the overall cyber risk strategy and goals? What is the timeline of such communication?	Who communicates on the overall cyber risk strategy and goals? What is the timeline of such communication?	None	Medium				
	Cyber Risk Performance Management Objectives	Performance Management	How do you influence and encourage senior management and employees to adhere to cyber security principles in day-to-day operations?	How do you influence and encourage senior management and employees to adhere to cyber security principles in day-to-day operations?	None	Medium				
		Cyber Risk Training	Is there a cyber risk training program in place?	Is there a cyber risk training program in place?	None	Medium				
	Cyber Awareness	General Cyber Risk Training	How does the program ensure that these messages are relevant and effective?	Please explain the programs and campaigns conducted to promote awareness of cyber security and cyber incidents across the enterprise?	None	Medium				
		Cyber Awareness	What channels are used to promote cyber awareness?	What channels are used to promote cyber awareness?	None	Medium				
	Reporting	Cyber Risk Disclosure & Reporting	When are cyber risks discussed with the board and senior management?	When are cyber risks discussed with the board and senior management?	None	Medium				
			Who are included in cyber risk disclosure?	Who are included in cyber risk disclosure?	None	Medium				

FIGURE 3.48 – Feuille des évaluations

3. Etude fonctionnelle et conceptuelle

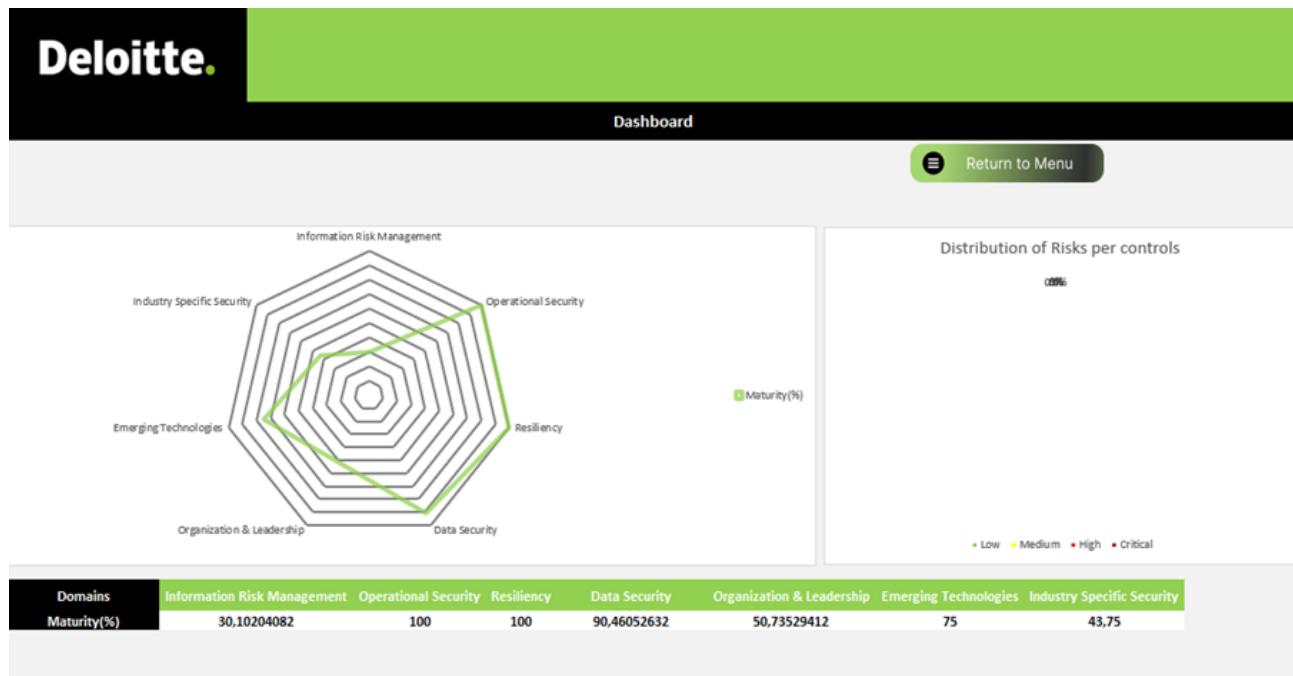


FIGURE 3.49 – Dashboard

5 Conclusion

Dans ce chapitre, nous avons présenté notre approche moderne de Cyber Due Diligence et ses processus de façon détaillée. Nous avons également présenté le Framework que nous avons réalisé tout en mettant l'accent sur la conception, l'alimentation des points de contrôle et l'automatisation des fonctionnalités. Dans le chapitre suivant, nous aborderons la partie pratique de notre projet, où nous allons présenter nos réalisations au niveau d'une mission client.

4

Mission Client

1 Introduction

Dans le présent chapitre, nous aborderons la mission d'accompagnement réalisée lors de mon stage, dans le contexte d'une mission d'assistance d'un client en fusions et acquisitions (M&A) et plus spécifiquement en Due Diligence et en Post-Due Diligence. Nous tenons à souligner que, en raison des obligations de confidentialité imposées par l'organisme d'accueil ainsi que de la sensibilité de notre client, nous ne pouvons pas fournir de détails spécifiques sur ma participation à cette mission. Cependant, cela ne nous empêche pas de consacrer ce chapitre à présenter notre rôle et les tâches que nous avons réalisées au sein de cette mission.

2 Contexte et objectifs

Au cours de mon stage au sein de Deloitte MCC, nous avons été impliqués dans une mission d'accompagnement en fusions et acquisitions pour un client français opérant dans le domaine de l'industrie électrique et des télécommunications. L'objectif de cette mission était d'assister le client à une opération d'acquisition et plus spécifiquement lors de l'acquisition d'une entreprise cible opérant dans le même secteur, mais dans un autre pays, tout en proposant la réalisation d'une due diligence approfondie de la cible en évaluant sa situation et sa posture cyber. Mon rôle consistait à soutenir l'équipe responsable de la due diligence en fournissant une approche et un Framework pour la partie Cyber qui vont aider ensuite à produire des analyses, des rapports et des recommandations pour aider notre client à prendre des décisions éclairées.

3 Contraintes

Il est important de souligner que, en raison de la nature confidentielle de la mission et des obligations légales de confidentialité, nous ne pouvons pas divulguer de détails spécifiques ni sur l'entreprise cible, ni sur les informations confidentielles auxquelles nous avons eu accès. Nous nous concentrerons donc d'une présentation générale des tâches et des résultats obtenus, tout en préservant la confidentialité des informations.

4 Méthodologie

La mission client se compose de deux volets distincts. Le premier volet concerne la phase de Due Diligence et l'évaluation de la posture de la cible par rapport à l'approche et l'outil

4. Mission Client

de Cyber Due Diligence que nous avons développé. Le deuxième volet se concentre sur la préparation pour la phase de Post-Deal Integration et Post-Merger Integration visant à fusionner harmonieusement les activités, les ressources et les processus des entreprises. Ce chapitre mettra principalement l'accent sur le premier volet suite à la finalisation de la phase de Due Diligence. Le deuxième volet n'était pas pris en compte lors de l'élaboration initiale de ce rapport puisqu'il est associé essentiellement à la finalisation de l'opération d'acquisition. Le positionnement de la mission dans le cycle MA ainsi que la méthodologie appliquée sont présentés ci-dessous :

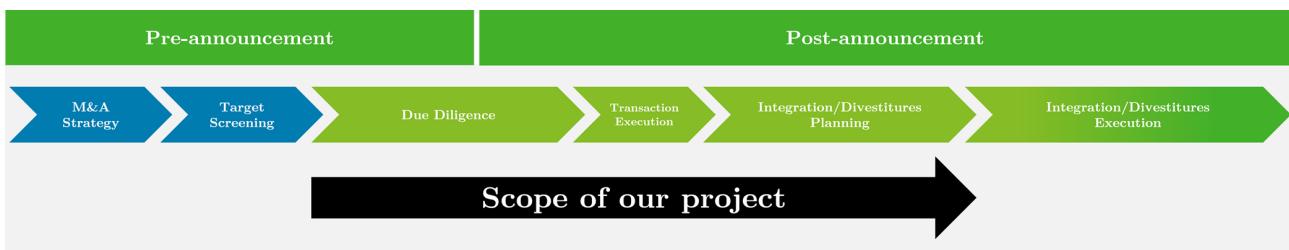


FIGURE 4.1 – Positionnement de la mission



FIGURE 4.2 – Méthodologie de la mission

5 Planning prévisionnel

Le planning prévisionnel de la mission a été établi en utilisant une approche méthodique basée sur les objectifs, les exigences et les livrables du projet. Le planning est divisé en deux volets distincts : Cyber Due Diligence et Post-Deal Integration Roadmap.

La mission a été officiellement lancée lors d'une réunion de kick-off le 20 avril et au moment de la rédaction de ce rapport, nous sommes à la dernière phase du premier volet.

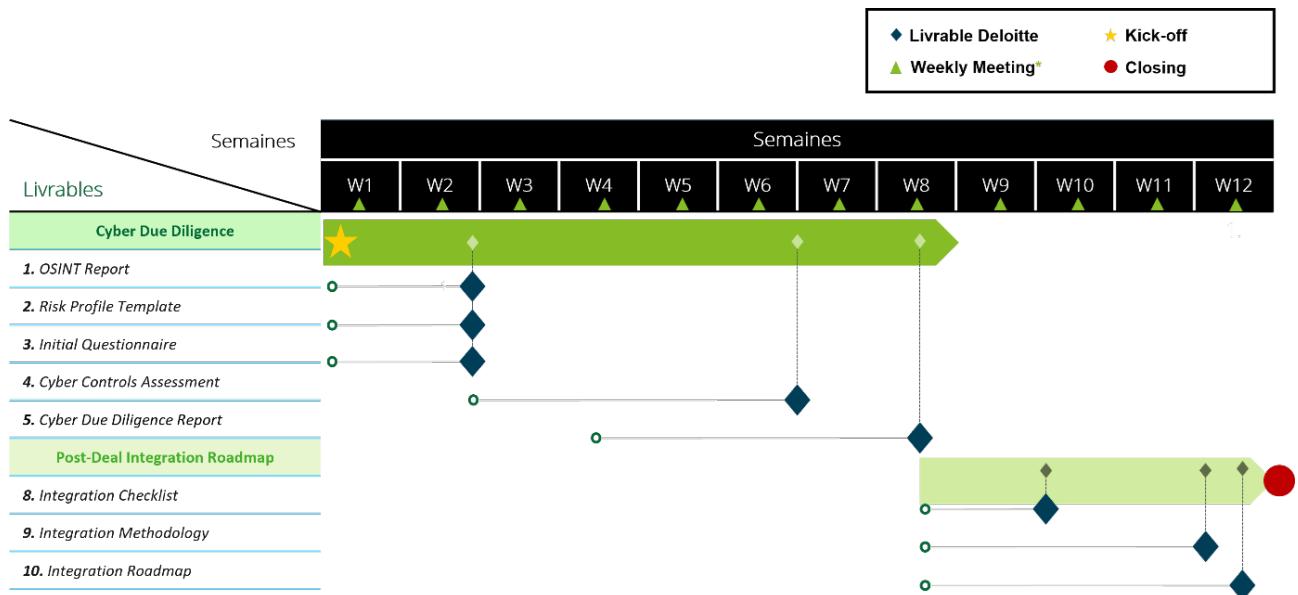


FIGURE 4.3 – Planning prévisionnel de mission

6 Application de notre approche et notre Framework

Comme indiqué dans la méthodologie, quatre des cinq étapes sont basées sur notre approche de la Cyber Due Diligence, et en ce qui concerne la cinquième étape, elle intervient directement après la finalisation de la transaction. À travers cette section, nous allons présenter en détail comment nous avons appliqué notre approche et notre Framework de Cyber Due Diligence ainsi que les principales étapes que nous avons suivies. Veuillez noter que certains détails spécifiques seront omis afin de préserver la confidentialité des entreprises impliquées.

6.1 Planification

Scope

4. Mission Client

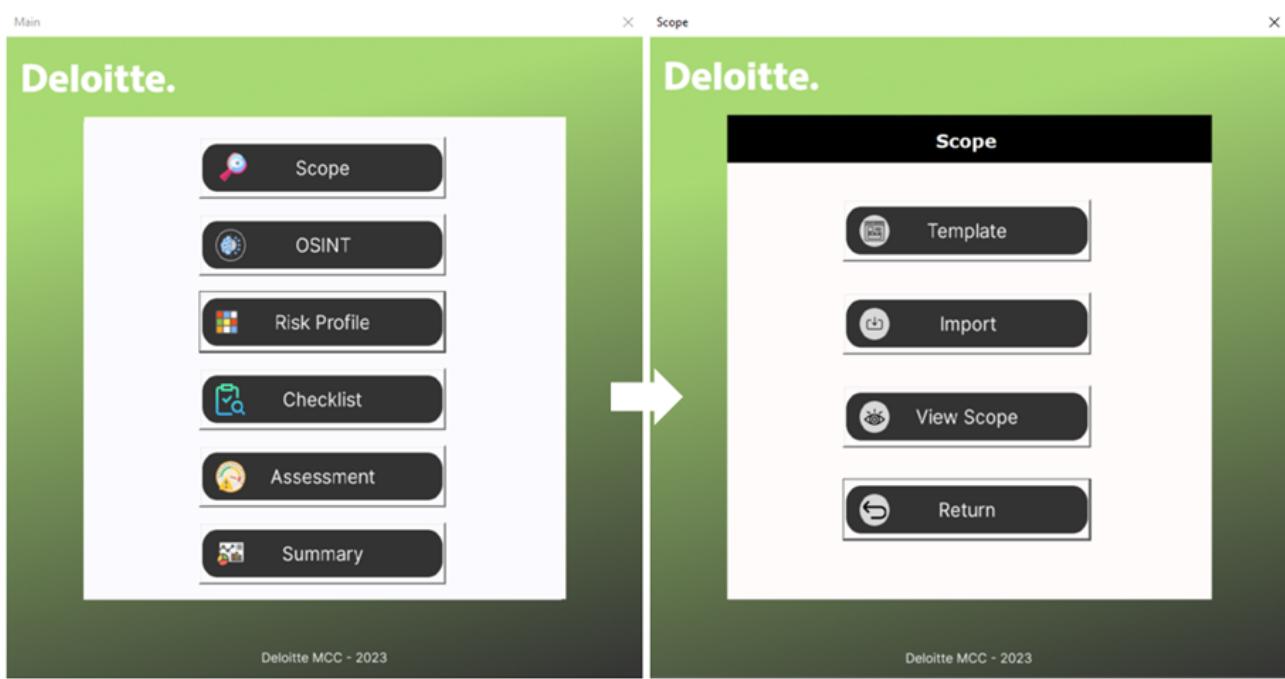


FIGURE 4.4 – Passage de la page d'accueil à la page Scope

Après génération de la Template de la phase de Scope et de planification, la Template est envoyée aux parties concernées pour qu'elle soit remplie en parallèle avec la collecte des données en OSINT et le questionnaire préliminaire.

Dans le contexte de la mission, l'évaluation des contrôles d'OT Security et du Software Security sont hors portée selon les exigences du client. La date initiale des évaluations était fixée du 20/04 au 26/05 en utilisant le Framework que nous avons conçu.

L'équipe de Cyber Due Diligence était constituée avec comme membres des consultants avec un background d'Audit de Sécurité pour les parties d'évaluation et un consultant Offensive Security pour le processus de collecte en OSINT.

Deloitte.

Engagement Setup

Return to Menu

Client:	
Target:	
Type of transaction:	Acquisition

Element	Purpose/Scope	Answer	Additional
Purpose	Specify the reason for conducting the cyber due diligence		
Limitations	Define the boundaries and limitations of the due diligence	OT and Legacy Software not included in the scope	
Scope	Clarify what systems, data, and processes are in scope for the assessment.	(as mentioned in Limitations)	
Timeline	Start and end date of the assessment	20/04/2023 to 26/05/2023	
Budget	Overall budget for the assessment, including any expected costs or expenses	*****	

FIGURE 4.5 – Feuille de Scope (1/2)

4. Mission Client

Assessment Criteria			
Element	Description	Answer	Additional answer
Criteria of evaluation	Define the criteria for evaluating the cybersecurity posture of the organization.	Comprendre les critères d'évaluation, les réglementations, les normes et les frameworks utilisés pour évaluer la posture de sécurité cyber de l'organisation.	
Regulations	Specify which regulations, standards, and frameworks will be used as the basis for the assessment.	Cyber Due Diligence Framework	Spécifier les réglementations, les normes et les frameworks utilisés comme base pour l'évaluation.
Requirements	Identify any specific requirements or guidelines for the assessment.	No OT/Software controls	Identifier les exigences spécifiques ou les directives pour l'évaluation.

Team		Number of members required	4
Role	Responsibilities	Required Skills	Member(s)
OSINT Collector		Offensive Security	
Data Reviewer		Audit	
Assessor		Audit	
Assessor		Audit	

FIGURE 4.6 – Feuille de Scope (2/2)

6.2 Collecte d'informations

OSINT

Source Name	Source Type	ID	Type of	Findings	Date of	Releva	Additional
[REDACTED]	Dark Web	DW-1	Data Leaks & Breaches	Discovery of confidential product designs publicly available on a file-sharing	24/04/2023	High	
[REDACTED]	Dark Web	DW-2	Data Leaks & Breaches	Unintentional exposure of internal operational documents	24/04/2023	High	
[REDACTED]	Dark Web	DW-3	Data Leaks & Breaches	Detection of customer databases or order records being openly accessible on unprotected web servers	24/04/2023	High	
[REDACTED]	Dark Web	DW-4	Data Leaks & Breaches	Identification of employee email addresses and passwords leaked in recent data	24/04/2023	High	
[REDACTED]	Breaches and Threat Intelligence	DW-5	Data Leaks & Breaches	Uncovering of compromised employee credentials	24/04/2023	High	
[REDACTED]	Web Forums	WF-1	Reputation	Discovery of blog posts regarding ethical issues associated with some of the company's operations	24/04/2023	High	
[REDACTED]	Public Records	PR-1	Reputation	Unveiling of some instances of regulatory violations involving the company	24/04/2023	High	

FIGURE 4.7 – Feuille d'OSINT

Le processus de collecte de renseignements en OSINT s'est déroulé sur une période d'une semaine, au cours de laquelle le Framework d'OSINT que nous avons conçu a été utilisé comme base pour l'approvisionnement des sources destinées aux outils internes d'OSINT existants. Plusieurs découvertes ont été réalisées, cependant, afin de préserver la confidentialité, nous ne détaillerons que de manière générale quelques-unes de ces découvertes, en protégeant ainsi l'anonymat des parties impliquées.

Parmi les découvertes, il a été constaté que des ports sensibles (tels que le partage de fichiers et l'administration) étaient exposés, ainsi que des erreurs de configuration au niveau de serveurs.

Par ailleurs, lors de la consultation de certains forums, des publications ont été découvertes, abordant des problèmes éthiques liés à certaines opérations de l'entreprise, ainsi que la révélation de violations réglementaires impliquant ladite entreprise. Bien que les détails spécifiques ne soient pas divulgués ici pour des raisons de confidentialité, ces découvertes soulignent la nécessité de prendre des mesures pour remédier à ces problèmes et garantir la conformité aux normes éthiques et réglementaires appropriées.

4. Mission Client

La découverte de designs de produits confidentiels disponibles publiquement sur une plate-forme de partage de fichiers a été un événement préoccupant pour l'entreprise. Cela a révélé une faille de sécurité majeure dans la protection des informations sensibles, exposant potentiellement la propriété intellectuelle de l'entreprise à des tiers non autorisés.

De plus, une exposition involontaire de documents opérationnels internes a été identifiée. Cela signifie que des informations confidentielles sur les procédures, les stratégies et les processus internes de l'entreprise étaient accessibles à des personnes non autorisées.

La détection de bases de données clients ou d'enregistrements de commandes accessibles ouvertement sur des serveurs Web non protégés a également été une découverte alarmante. Cela a exposé des données personnelles sensibles, telles que les coordonnées des clients et les informations de commande, à un risque de compromission et d'utilisation abusive.

L'identification de quelques adresses e-mail et de mots de passe d'employés divulgués lors de récentes violations de données a été une autre préoccupation majeure. Cela a exposé les comptes des employés à des risques de piratage et d'accès non autorisé.

Les découvertes réalisées mettent en évidence les vulnérabilités présentes dans la posture de sécurité de la cible, et elles serviront de base lors de la personnalisation des mesures d'évaluation. Une attention particulière sera accordée aux domaines liés aux données sensibles et à la protection de la propriété intellectuelle.

Questionnaire préliminaire

Après avoir mené des entretiens avec les parties prenantes de l'entité cible, nous avons pu recueillir des réponses aux 25 questions du questionnaire préliminaire. Ces réponses ont joué un rôle clé dans la définition précise de la portée de notre évaluation et des prochaines étapes à suivre.

Grâce à ces réponses, nous avons pu constater que les systèmes ICS et SCADA de la cible se situent en dehors de notre champ d'évaluation. De plus, il a été révélé que la cible n'utilise pas de services Cloud et n'est pas engagée dans des activités de développement logiciel.

En ce qui concerne les données traitées, nous avons identifié que la cible détient des données personnelles PII, des données financières ainsi que des propriétés intellectuelles. Toutefois, il est important de noter que les réponses de la cible indiquent qu'aucune fuite de données n'a été subie jusqu'à présent, bien que cela contredise les informations que nous avons obtenues grâce à l'OSINT (Open Source Intelligence).

Ces réponses fournies par la cible nous permettent de personnaliser la liste des contrôles qui

4. Mission Client

seront évalués. En tenant compte de ces informations, nous pourrons nous concentrer sur les domaines spécifiques liés à la protection des données personnelles, des finances et des propriétés intellectuelles, tout en veillant à prendre en compte les possibles vulnérabilités révélées par l'OSINT malgré les réponses initiales.

The screenshot shows a Deloitte questionnaire titled "Initial Questionnaire". The form includes a header with the Deloitte logo and a "Return to Menu" button. The main section contains a table with 25 rows of questions and answers. The columns are: "Question #", "Question", "Question type", "Answer", and "Notes". The "Notes" column for question 4 indicates "Out of Scope". The "Notes" column for question 15 lists "Intellectual property", "Financial data", and "Personal identifiable information (PII)".

Question #	Question	Question type	Answer	Notes
1	What type of business does your organization conduct?	Open Question	Manufacturing	
2	How many employees does your organization have?	Open Question		300
3	What is the size of your organization's IT infrastructure?	Open Question	Small	
4	Does your organization use any industrial control systems (ICS) or supervisory control and data acquisition (SCADA) systems in your operations?	Yes/No	No	Out of Scope
5	Is there a cybersecurity department within the organization?	Yes/No	Yes	
6	Does your organization outsource any security functions to third-party service providers?	Yes/No	Yes	
7	Has your organization ever experienced a significant cybersecurity incident?	Yes/No	No	
8	Does your organization maintain an inventory of all hardware and software assets?	Yes/No	No	
9	Does your organization have a formal security policy in place?	Yes/No	Yes	
10	What types of cybersecurity policies do you have in place in your organization today?	Open Question	Yes	
11	Does your organization use cloud services?	Yes/No	No	
12	Does your organization develop custom software applications?	Yes/No	No	
13	Does your organization have a process in place for managing software patches and updates?	Yes/No	No	
14	Does your organization process or store sensitive information?	Yes/No	Yes	
15	What type of sensitive information does your organization process or store?	Multiple Choice (PII)	Intellectual property Financial data Personal identifiable information (PII)	
16	Does your organization have a disaster recovery plan?	Yes/No	Yes	
17	Does your organization have an incident response plan?	Yes/No	Yes	
18	Does your organization have a data retention policy?	Yes/No	No	
19	Does your organization have a third-party risk management program?	Yes/No	No	
20	Does your organization have a compliance program in place?	Yes/No	No	
21	Does your organization have a risk management program in place?	Yes/No	Yes	
22	Has your organization ever experienced a security breach?	Yes/No	No	
23	Has your organization ever conducted a security assessment or audit?	Yes/No	Yes	
24	Does your organization have a security awareness training program for employees?	Yes/No	No	
25	Does your organization perform background checks on employees and contractors?	Yes/No	No	

FIGURE 4.8 – Questionnaire rempli

Profils de risques

4. Mission Client

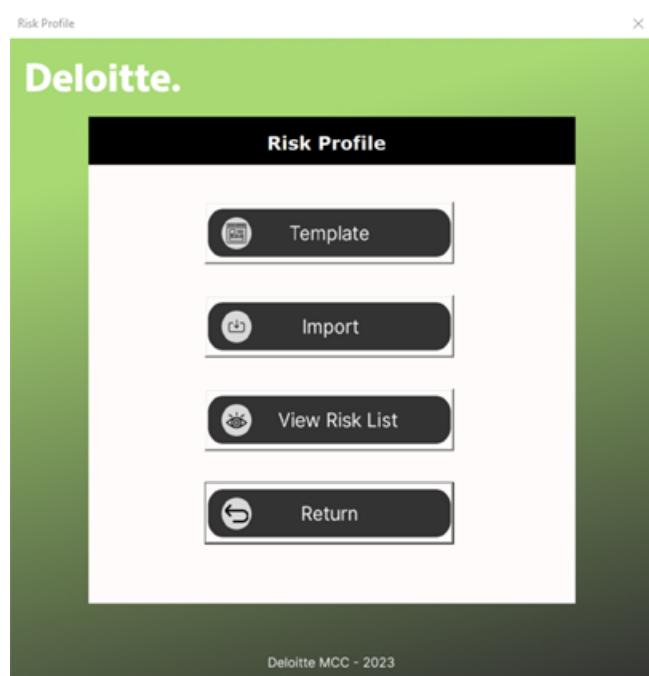


FIGURE 4.9 – Page de risques

Une fois les modèles générés, ils ont été envoyés aux parties prenantes de la cible ainsi qu'aux clients afin qu'ils les remplissent avec les risques identifiés propres à chaque entité.

4. Mission Client

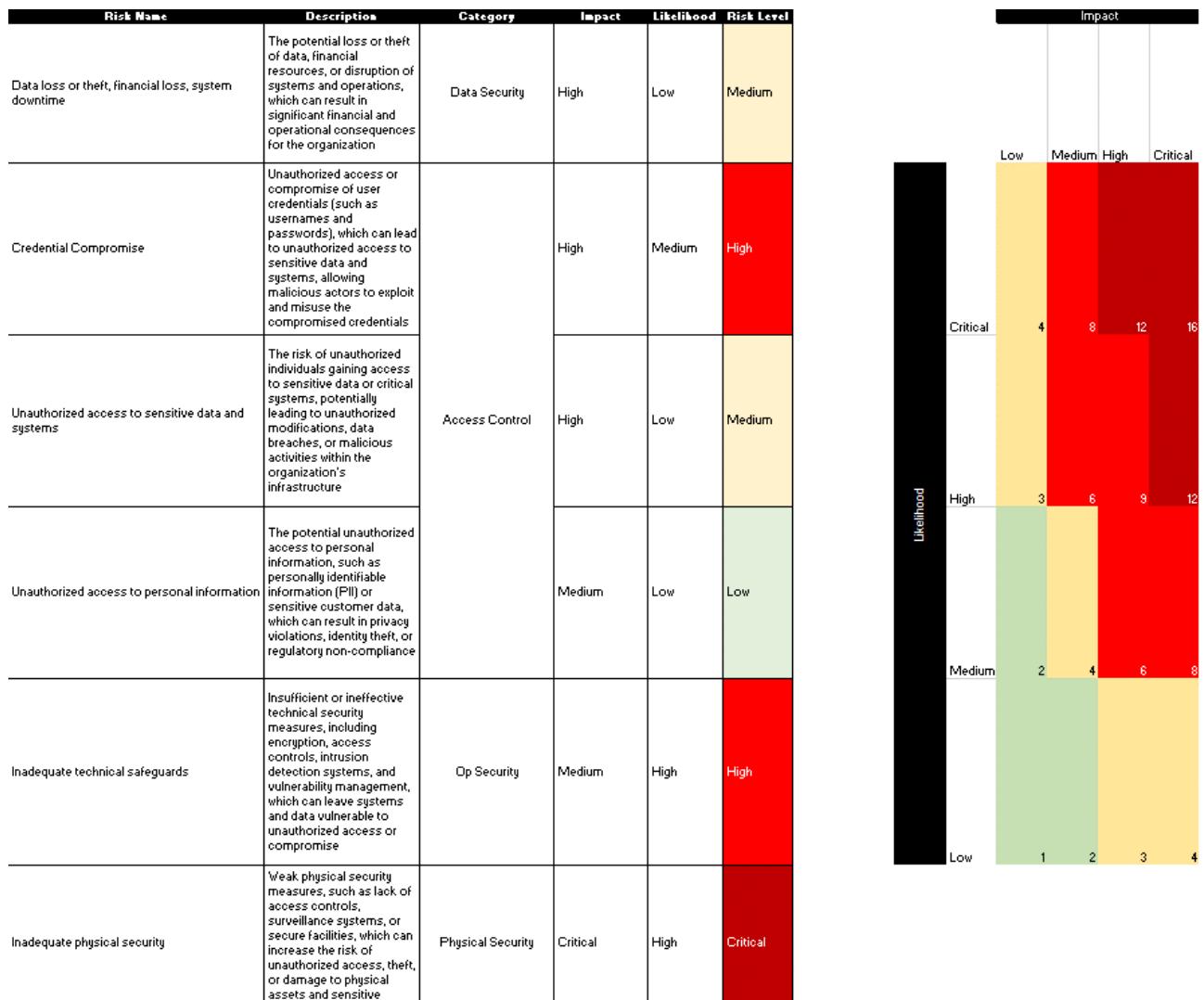


FIGURE 4.10 – Aperçu du profil de risque de la cible

4. Mission Client

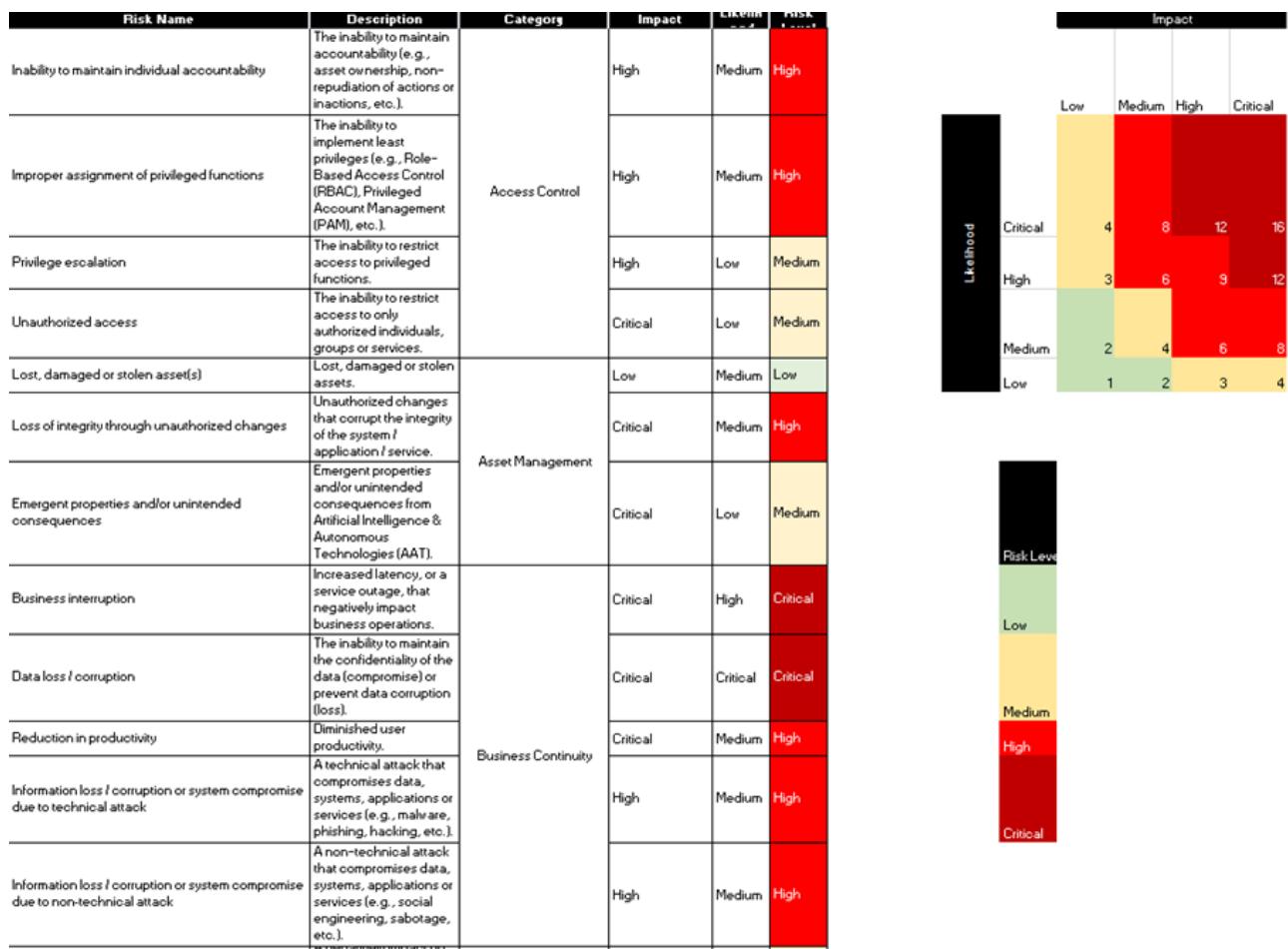


FIGURE 4.11 – Aperçu du profil de risque du client

4. Mission Client

Nous avons observé que le profil de risques du client est plus avancé et détaillé, comprenant 50 risques identifiés dans plusieurs domaines, par rapport au profil de la cible qui ne compte que 17 risques généraux. Cette différence peut être attribuée à la taille et au chiffre d'affaires de chaque entité. Nous avons également constaté des risques communs entre les deux, mais avec des niveaux de risques différents. Voici quelques exemples des risques communs :

- Risque A : Compromission d'identifiants

Credential Compromise	Unauthorized access or compromise of user credentials (such as usernames and passwords), which can lead to unauthorized access to sensitive data and systems, allowing malicious actors to exploit and misuse the compromised credentials.	Access Control	Critical	Critical	Critical
-----------------------	--	----------------	----------	----------	----------

FIGURE 4.12 – Risque A chez le client

Credential Compromise	Unauthorized access or compromise of user credentials (such as usernames and passwords), which can lead to unauthorized access to sensitive data and systems, allowing malicious actors to exploit and misuse the compromised credentials	High	Medium	High
-----------------------	---	------	--------	------

FIGURE 4.13 – Risque A chez la cible

- Risque B : Perte, dommage ou vol des actifs

Lost, damaged or stolen asset(s)	Lost, damaged or stolen assets.	Low	Medium	Low
----------------------------------	---------------------------------	-----	--------	-----

FIGURE 4.14 – Risque B chez le client

4. Mission Client

Lost, damaged or stolen asset(s)	Lost, damaged or stolen assets.	Access Control	Critical	Critical	Critical
----------------------------------	---------------------------------	----------------	----------	----------	----------

FIGURE 4.15 – Risque B chez la cible

Il est évident que chaque entité accorde une priorité différente à ses risques en fonction de son contexte. Par exemple, en ce qui concerne les pertes d'actifs, l'entité cible, en raison de sa petite taille et du nombre limité de ses actifs, considère l'impact comme étant critique, tandis que l'entité cliente qualifie ce risque comme étant modéré.

L'étape suivante consiste à importer les deux profils dans notre outil, ce qui est accompli d'un simple clic. Une fois les profils importés, ils sont fusionnés pour obtenir un profil de risque consolidé, dans lequel les priorités des risques sont calculées automatiquement à l'aide des algorithmes mis en place. En cas de risques communs, la priorité choisie est la plus élevée entre les deux profils.

Risk Name	Category	Description	Priority
Inability to maintain individual accountability	Access Control	The inability to maintain accountability (e.g., asset ownership, non-repudiation of actions or inactions, etc.).	High
Improper assignment of privileged functions		implement least privileges (e.g., Role-Based Access Control (RBAC), Privileged Account Management (PAM), etc.).	High
Privilege escalation		The inability to restrict access to privileged functions.	Medium
Unauthorized access		The inability to restrict access to only authorized individuals, groups or services.	Medium
Lost, damaged or stolen asset(s)	Asset Management	Lost, damaged or stolen assets.	Critical
Loss of integrity through unauthorized changes		Unauthorized changes that corrupt the integrity of the system / application / service.	High
Emergent properties and/or unintended consequences		Emergent properties and/or unintended consequences from Artificial Intelligence & Autonomous Technologies (AAT).	Medium
Business interruption	Business Continuity	Increased latency, or a service outage, that negatively impact business operations.	Critical
Data loss / corruption		The inability to maintain the confidentiality of the data (compromise) or prevent data corruption (loss).	Critical
Reduction in productivity		Diminished user productivity.	High
		A technical attack that compromises data, systems, applications or	

FIGURE 4.16 – Profil consolidé

4. Mission Client

Revenant aux deux exemples des risques communs, nous constatons que les priorités ont été modifiées après consolidation.

Credential Compromise	Access Control	compromise of user credentials (such as usernames and passwords), which can lead to unauthorized access to sensitive data and systems, allowing malicious actors to exploit and misuse the compromised credentials	Critical
-----------------------	----------------	--	----------

FIGURE 4.17 – Risque A consolidé

Lost, damaged or stolen asset(s)	Asset Management	Lost, damaged or stolen assets.	Critical
----------------------------------	------------------	---------------------------------	----------

FIGURE 4.18 – Risque B consolidé

6.3 Réalisation des évaluations

Une fois les étapes précédentes complétées, telles que la définition du périmètre, la collecte de renseignements en OSINT, la consolidation des profils de risques et le questionnaire préliminaire, nous obtenons un Framework d'évaluation personnalisé qui est adapté au contexte et aux besoins spécifiques de la mission. En tenant compte des limitations identifiées ainsi que des découvertes réalisées, notre Framework a été optimisé, passant de 587 points de contrôle répartis dans 7 domaines majeurs à 436 points de contrôle répartis dans 6 domaines.

Cette réduction du nombre de points de contrôle a été effectuée en tenant compte des spécificités de la mission et en éliminant les domaines et sous-domaines non pertinents tels que les sous-domaines de OT Security, Payment Card Information Security et Protected Health Information Security entre autres. Ainsi, nous avons pu concevoir un Framework d'évaluation plus ciblé et efficace, en se concentrant sur les aspects les plus pertinents pour évaluer les risques et la sécurité de la cible.

Cette personnalisation du Framework d'évaluation permet de mieux répondre aux besoins spécifiques de la mission, en fournissant une approche plus concise et focalisée sur les enjeux critiques. Il s'agit d'une étape importante pour assurer une évaluation rigoureuse et pertinente de la sécurité de la cible, en prenant en compte les ressources disponibles, les contraintes et les priorités identifiées tout au long du processus.

Domaines concernés

Après avoir établi la portée de l'évaluation, les sous-domaines du Cloud, de l'OT et de la sécurité des logiciels ont été automatiquement exclus. De plus, suite à l'analyse du questionnaire préliminaire, les sous-domaines de PHI (informations de santé protégées) et de PCI (normes de sécurité des données des cartes de paiement) ont été éliminés.

L'évaluation est réalisée sur les 6 Domaines restants :

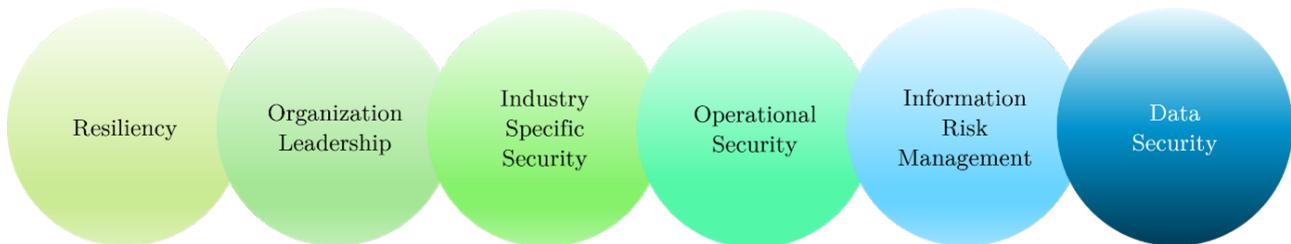


FIGURE 4.19 – Domaines de la mission

Exemples d'évaluation

Business Recovery	Describe the enterprise level recovery strategy that are in the place. What is the scope of business recovery?	Business interruption	Critical	The enterprise-level recovery strategies are poorly defined and lack a clear scope of business recovery. There is no comprehensive plan in place to address different scenarios and ensure the continuity of critical business functions.	1. Poor	Business Continuity Plan
Recovery Architectures	How is the recovery architecture designed and implemented?	Business interruption	Critical	The recovery architecture is poorly designed and implemented. There is a lack of proper infrastructure and technology to support efficient recovery processes. The organization relies on manual interventions, resulting in delays and inefficiencies.	1. Poor	Business Continuity Plan
Automation Capabilities	What automation and predictive failure techniques are used to support recovery processes?	Business interruption	Critical	The organization has minimal automation and predictive failure techniques in place to support recovery processes. There is a limited use of advanced technologies and predictive analytics, which hinders the organization's ability to respond effectively to disruptions and failures.	2. Fair/Partially Effective	Business Continuity Plan

FIGURE 4.20 – Exemple de 3 contrôles de Resiliency

4. Mission Client

Control Effectiveness Assessment										 Return to Menu
Theme	Statement	Risk(s) Addressed	Risk Priority	Answer	Control Effectiveness	Evidence	Notes	Owner	Status	Due Date
Awareness	How are business continuity activities reported and communicated across business units?	Business interruption	Critical	The organization has no established mechanism for reporting and communicating business continuity activities across business units. Information is shared sporadically through informal channels, leading to inconsistent and incomplete communication.	1 Poor				Completed	
Planning and Testing	What are the mechanisms being used to test and assess your BCPs?	Business interruption	Critical	The organization relies on outdated and ad-hoc methods for testing and assessing Business Continuity Plans (BCPs). There is no formalized process in place, resulting in inadequate testing and assessment of the plans' effectiveness.	1 Poor				Completed	
Business Recovery	Describe the enterprise-level recovery strategies that are in place. What is the scope of business recovery?	Business interruption	Critical	The enterprise-level recovery strategies are poorly defined and lack a clear scope of business recovery. There is no comprehensive plan in place to address different scenarios and ensure the continuity of critical business functions.	1 Poor				Completed	
Recovery Architectures	How is the recovery architecture designed and implemented?	Business interruption	Critical	The recovery architecture is poorly designed and implemented. There is a lack of proper infrastructure and technology to support efficient recovery processes. The organization relies on manual interventions, resulting in delays and inefficiencies.	1 Poor				Completed	
Automation Capabilities	What automation and predictive failure techniques are used to support recovery processes?	Business interruption	Critical	The organization has minimal automation and predictive failure techniques in place to support recovery processes. There is a limited use of advanced technologies like machine learning and analytics, which hinders the organization's ability to respond effectively to disruptions and failures.	2 Fairly Partially Effective				Completed	

FIGURE 4.21 – L'exemple dans la feuille

En raison des considérations de confidentialité, nous avons pris la décision de nous concentrer sur des exemples spécifiques issus d'un seul domaine, à savoir la résilience. Cela nous permet de préserver la confidentialité des informations sensibles tout en illustrant de manière concrète les défis et les mesures prises dans ce domaine particulier.

Dans les trois exemples, il s'agit du sous-domaine de Business Continuity Disaster Recovery et plus particulièrement le thème de Business Continuity Plan. Le risque associé à ces trois points de contrôle est le risque d'interruption des activités avec un niveau de priorité critique.

L'évaluation montre que les stratégies de reprise au niveau de l'entreprise sont mal définies et manquent d'une portée claire pour la reprise des activités. Il n'existe aucun plan global pour faire face à différents scénarios et assurer la continuité des fonctions essentielles de l'entreprise. Cette lacune se traduit par un niveau d'efficacité faible dans "Business Recovery".

L'architecture de récupération est également mal conçue et mise en œuvre, avec un manque d'infrastructure et de technologie adéquates pour soutenir les processus de récupération efficaces. L'organisation dépend d'interventions manuelles, ce qui entraîne des retards et des inefficacités. Dans la catégorie "Recovery Architectures", le niveau d'efficacité des contrôles est faible.

De plus, les capacités d'automatisation et les techniques de détection des pannes sont limitées, ce qui affecte la capacité de l'organisation à réagir efficacement aux perturbations et aux défaillances. Dans l'ensemble, l'évaluation indique un niveau d'efficacité partialement efficace d'où un besoin d'amélioration significative dans la mise en place d'un plan de continuité des activités et l'utilisation de technologies avancées pour soutenir les processus de récupération.

6.4 Résultats

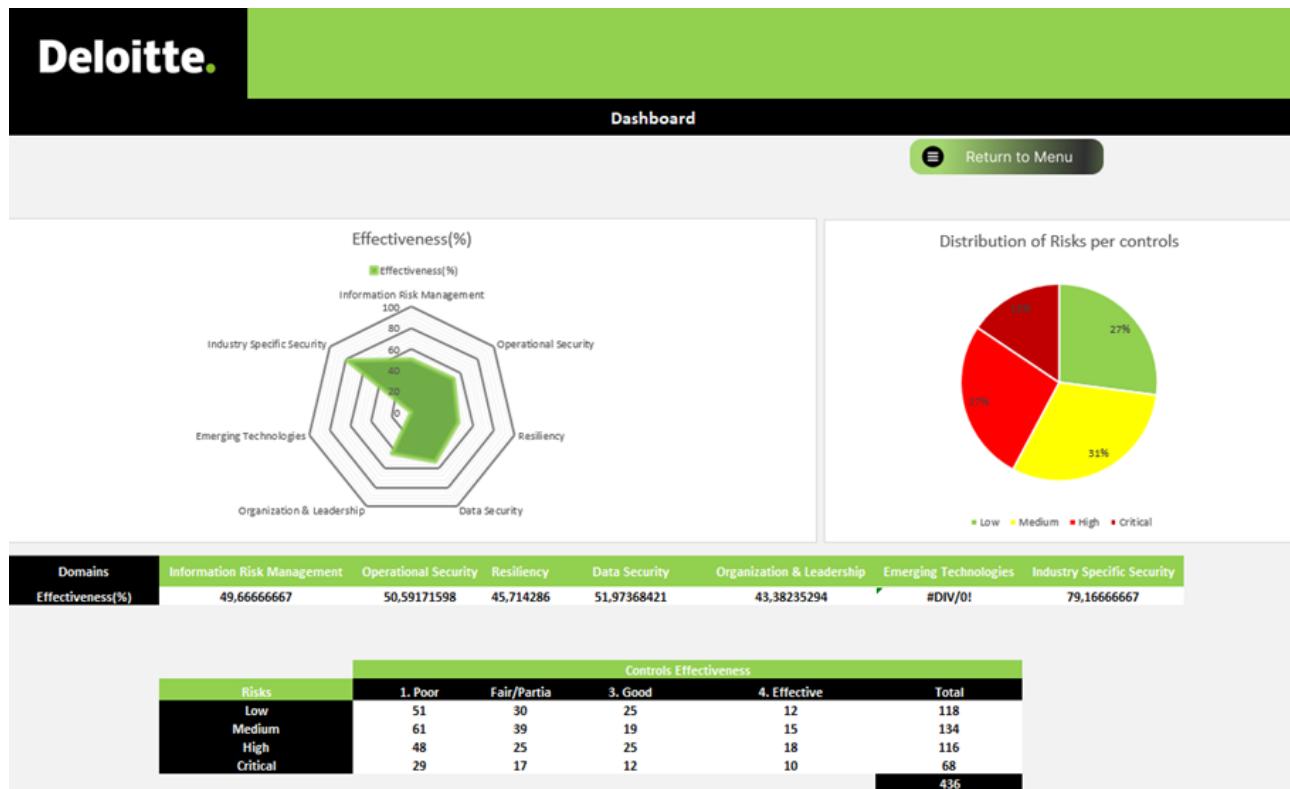


FIGURE 4.22 – Feuille Dashboard

Les résultats de l'évaluation sont présentés à travers une série de graphiques visuels dans la feuille de Dashboard pour mieux illustrer les performances des contrôles dans chaque domaine. Le premier graphique est un graphe radar qui présente les pourcentages d'efficacité des contrôles dans chaque domaine. Cela nous permet de visualiser globalement les domaines qui ont obtenu les meilleurs résultats en termes d'efficacité des contrôles.

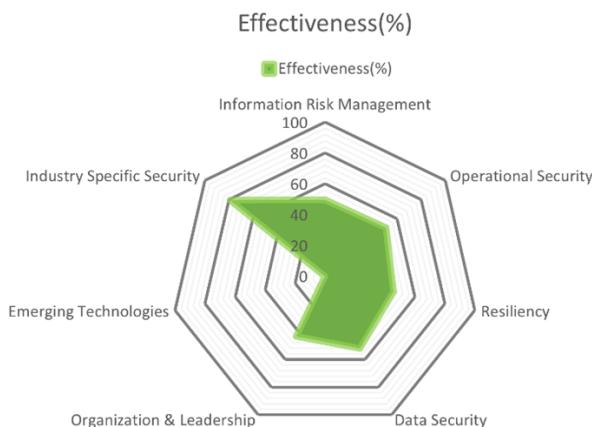


FIGURE 4.23 – Graphe Radar des pourcentages d'efficacité

L'analyse des résultats de l'évaluation montre que les domaines de « Information Risk Management » et « Operational Security » ont obtenu des pourcentages d'efficacité relativement

4. Mission Client

proches, soit 49,67% et 50,59% respectivement. Cela indique une efficacité partielle des points de contrôles vis-à-vis aux risques associés dans ces domaines.

Domaines	Information Risk Management	Operational Security	Resiliency	Data Security	Organization & Leadership	Industry Specific Security
Efficacité (%)	49,67	50,59	45,71	51,97	43,38	79,16

FIGURE 4.24 – Les pourcentages d'efficacité des domaines

Le domaine de « Data Security » a obtenu un pourcentage d'efficacité de 51,97%, ce qui est légèrement supérieur à la moyenne et qui indique aussi que les contrôles du domaine sont toujours partiellement efficaces.

Les domaines de « Organization Leadership » et « Resiliency » ont obtenu les pourcentages d'efficacité les plus bas, avec 43,38% et 45,71% respectivement. Cela suggère que des améliorations significatives sont nécessaires pour renforcer la gestion organisationnelle et la résilience en termes de sécurité.

Enfin, le domaine de « Industry Specific Security » a montré le pourcentage d'efficacité le plus élevé, avec 79,17%. Ce qui est généralement dû à l'élimination des sous-domaines de PHI et PCI et l'évaluation d'un seul sous-domaine qui est la sécurité de la propriété intellectuelle. Cela indique aussi que des mesures de sécurité spécifiques à ce dernier sous-domaine, reflétant une performance solide des points de contrôle.

4. Mission Client



FIGURE 4.25 – Efficacité par domaine

De plus, pour chaque domaine, nous avons des graphiques à barres détaillés qui montrent l'efficacité des contrôles spécifiques à ce domaine et qui fournissent une vue détaillée des performances des contrôles dans chaque domaine.

4. Mission Client

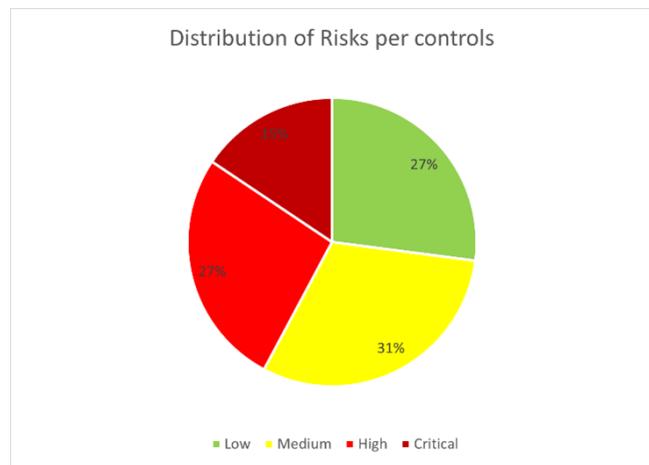


FIGURE 4.26 – Distribution des risques

Ensuite, nous avons un graphique en camembert qui présente la distribution des niveaux de risques identifiés. Cette représentation graphique permet de visualiser la répartition des risques entre les différentes catégories (Faible, modéré, élevé et critique), ce qui facilite l'identification des niveaux de risques les plus préoccupants.

Risques	Efficacité des contrôles				
	Médiocre	Efficace partiellement	Bon	Efficace	Total
Faible	51	30	25	12	118
Modéré	61	39	19	15	134
Elevé	48	25	25	18	116
Critique	29	17	12	10	68
					436

FIGURE 4.27 – Distribution détaillée des risques

4. Mission Client

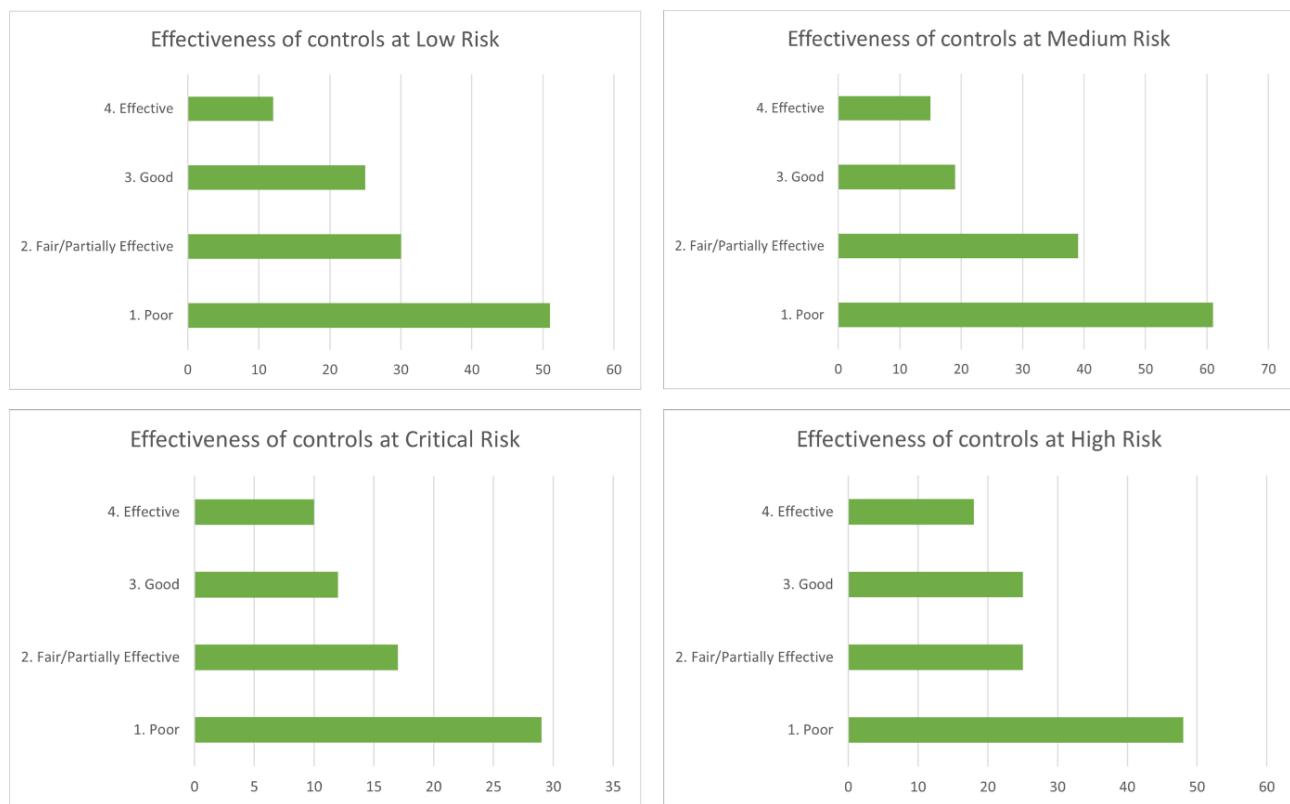


FIGURE 4.28 – Niveau d'efficacité par niveau de risque

L'analyse des résultats de ce tableau et des graphes associés montre une répartition inégale.

Voici les observations clés :

- Pour les risques faibles, la majorité des contrôles sont classés comme "Médiocre" (51) et "Efficace partiellement" (30). Cependant, il y a aussi un nombre significatif de contrôles classés comme "Bon" (25) et "Efficace" (12). Cela suggère qu'il faut renforcer l'efficacité des contrôles face aux risques faibles.
- Pour les risques modérés, on observe une légère dominance des contrôles classés comme "Médiocre" (61) et "Efficace partiellement" (39), tandis que les contrôles classés comme "Bon" (19) et "Efficace" (15) sont peu présents. Cela indique qu'il y a une grande marge de progression pour améliorer l'efficacité des contrôles face aux risques modérés.
- Pour les risques élevés, les contrôles sont répartis de manière relative entre les catégories "Médiocre" (48), "Efficace partiellement" (25), "Bon" (25) et "Efficace" (18). Cela suggère que seulement 37% (43 contrôles sur 116) sont satisfaisants face aux risques élevés, ce qui est inacceptable et nécessite des actions correctives immédiates.
- Pour les risques critiques, on observe une prédominance des contrôles classés comme "Médiocre" (29) et "Efficace partiellement" (17) avec une présence plus petite des contrôles classés comme "Bon" (12) et "Efficace" (10). Cela souligne l'importance d'accorder une attention prioritaire aux risques critiques et de mettre en place des mesures de contrôle

plus solides pour les atténuer.

En conclusion, les résultats mettent en évidence la nécessité d'améliorer l'efficacité des contrôles dans tous les niveaux de risques, avec une attention particulière aux risques critiques et élevés.

Au total, nous avons présenté 12 graphes ainsi que 2 tableaux qui offrent une vue complète et détaillée des résultats de l'évaluation, permettant une analyse approfondie des performances des contrôles dans chaque domaine et par rapport aux niveaux de risques associés.

7 Conclusion

A travers ce chapitre, nous avons pu mettre en évidence notre rôle et les tâches que nous avons accomplies tout au long d'une mission client. Grâce à cette mission, nous avons eu la chance de mettre en pratique l'approche que nous avons conçue et d'utiliser le Framework et l'outil associés à cette approche.

Conclusion générale et perspectives

La convergence de la technologie et le monde des affaires se confrontent aux réalités des risques cybersécuritaires, notamment lors des transactions de fusions et acquisitions. Les opportunités stratégiques offertes par ces transactions permettent aux entreprises d'étendre leur portée, d'accroître leur compétitivité et de réaliser des synergies. Cependant, ce processus implique souvent l'intégration de systèmes informatiques, de réseaux et de données, ce qui accroît leur exposition aux risques cybersécuritaires.

C'est dans ce contexte-là que mon projet effectué au sein de l'équipe Cyber Stratégie de Deloitte Morocco Cyber Center opère. Ce dernier consiste à concevoir une approche moderne de Cyber Due Diligence avec son propre Framework holistique avant de les mettre en œuvre dans le cadre d'une mission client.

En effet, Deloitte fournit des services de bout en bout dans les missions et projets d'assistance aux clients en M&A, allant de proposition de stratégie en M&A jusqu'à l'exécution d'intégration. Dans ce sens, pour le compte d'un client, Deloitte vise à fournir une assistance optimale au client lors de la phase de Due Diligence en Pré-Deal en exploitant des approches modernes et des Frameworks personnalisables afin d'évaluer de manière holistique la posture cybersécuritaire de l'entité cible.

Dans cette perspective, nous avons procédé d'abord à une étude et analyse des processus de M&A existants ainsi que des normes et cadres éprouvés de sécurité. Nous avons ensuite recensé les besoins des clients potentiels en addition des tendances de cybersécurité en M&A pour concevoir une approche moderne axée sur les risques de Cyber Due Diligence avec son propre Framework automatisé. Enfin, nous avons mis en œuvre nos réalisations dans le contexte de la mission pour évaluer une entité cible de façon approfondie et proposer des recommandations stratégiques pertinentes au client.

Grâce à la solide méthodologie de travail acquise auprès de Deloitte et à ma formation, j'ai

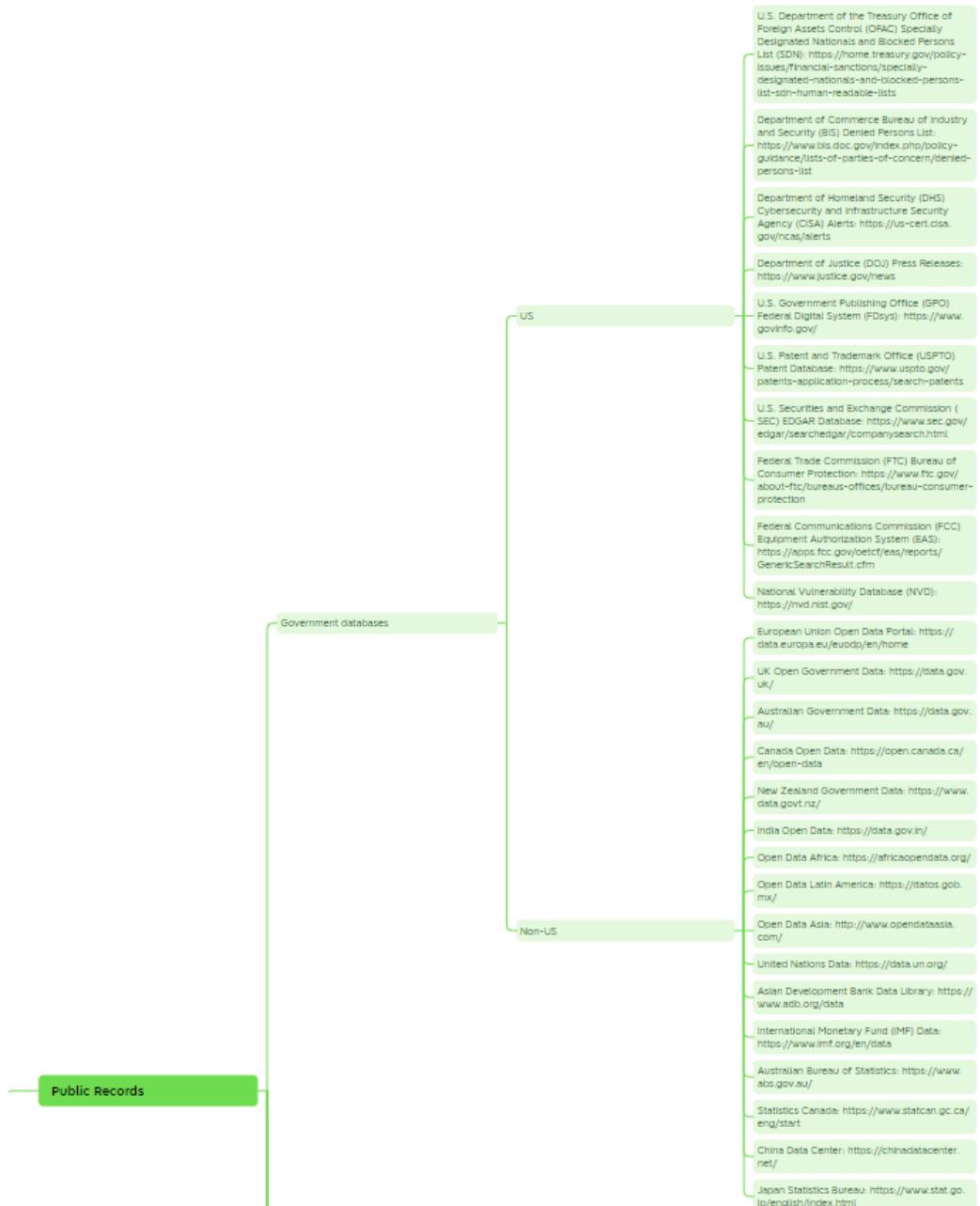
pu apporter une contribution précieuse à l'amélioration des processus de Cyber Due Diligence. En facilitant les tâches des consultants et des évaluateurs grâce à la nature automatisée de nos réalisations, j'ai pu rendre le processus plus efficace et efficient.

Certains détails et améliorations n'ont pas pu être abordés dans le cadre de ce projet, ouvrant ainsi la voie à de nombreuses perspectives à explorer dans un avenir proche. Ces perspectives permettront d'améliorer davantage le service de Cyber M&A offert par Deloitte à ses clients, en particulier :

- La génération automatique des recommandations en termes de stratégie d'intégration pour chaque domaine et sous-domaine en se basant sur les résultats des évaluations.
- L'association de notre Framework à d'autres cadres réglementaires pour évaluer la conformité de la cible à chaque réglementation concernée
- La création d'un outil automatisée basé sur notre Framework d'OSINT permettant une génération automatique des rapports sur les entités cibles.

A

Annexes



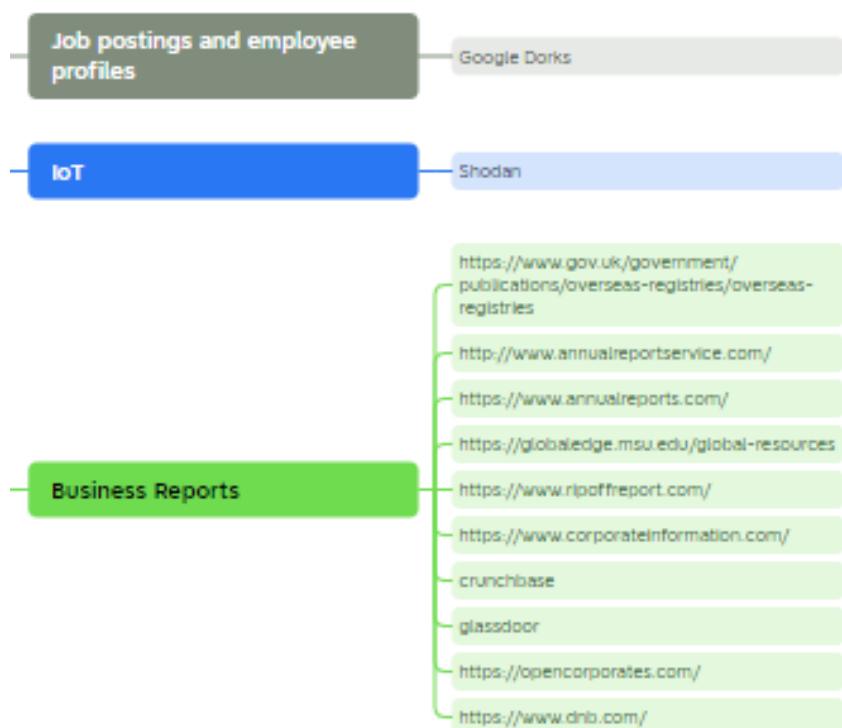
OSINT FRAMEWORK (1/4) - GOVERNMENT DATABASES



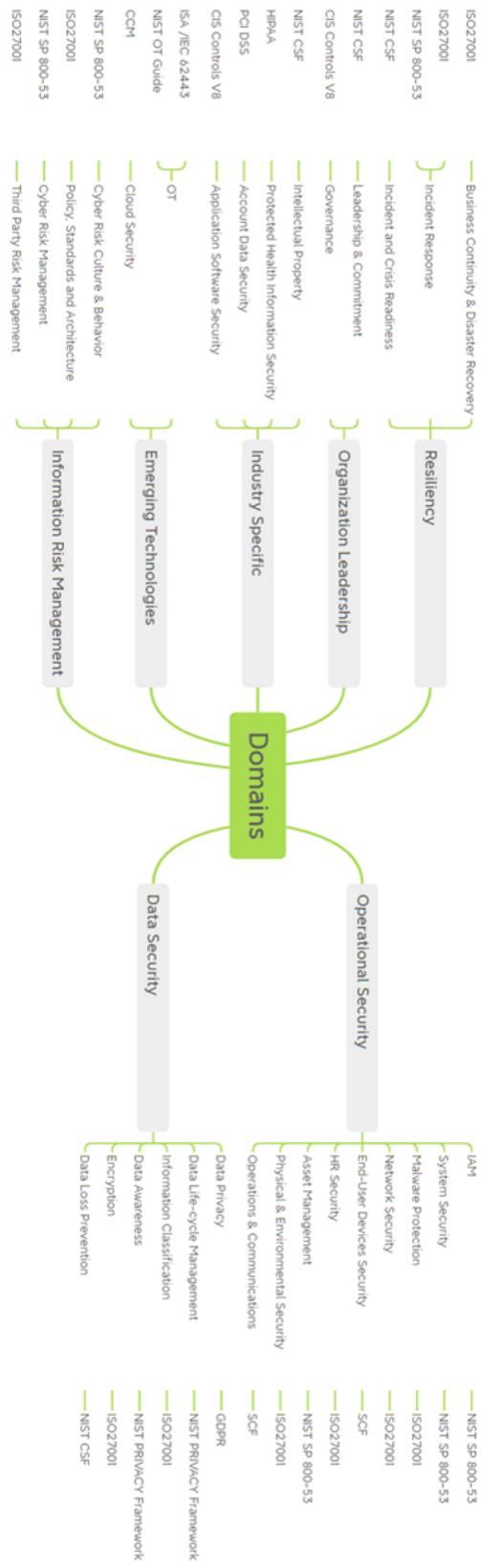
OSINT FRAMEWORK (2/4)



OSINT FRAMEWORK (3/4)



OSINT FRAMEWORK (4/4)



Mapping global

```
Private Sub AssBtn1_Click()
ThisWorkbookActivate
Application.Visible = True
Sheet3.Activate
Unload Mainform
End Sub

Private Sub CommandButton3_Click()
Me.hide
ScopeForm.Show
Unload Mainform
End Sub
Private Sub CommandButton4_Click()
Me.hide
OSINTForm.Show
End Sub

Private Sub CommandButton5_Click()
Me.hide
CheckForm.Show
End Sub

Private Sub riskprobtn_Click()
Me.hide
RiskForm.Show
End Sub

Private Sub SumBtn1_Click()
Me.hide
SumForm.Show
End Sub
```

PROGRAMME DE LA PAGE D'ACCEUIL

```

Private Sub GeneratetempBtn_Click()

    Dim ws1 As Worksheet
    Dim ws2 As Worksheet
    Dim wb As Workbook
    Dim filename As String
    Dim counter1, counter2 As Integer

    Set wb = ThisWorkbook ' set the workbook to the active workbook
    Set ws1 = wb.Sheets("Sheet1") ' set the first worksheet that you want to save
    Set ws2 = wb.Sheets("Sheet2") ' set the second worksheet that you want to save

    If ws1.Visible = xlSheetHidden Then
        ws1.Visible = xlSheetVisible
        counter1 = 1
    Else
        counter1 = 0
    End If

    If ws2.Visible = xlSheetHidden Then
        ws2.Visible = xlSheetVisible
        counter2 = 1
    Else
        counter2 = 0
    End If
    ' get the file name from the user
    filename = Application.GetSaveAsFilename(fileFilter:="Excel Files (*.xlsx), *.xlsx")

    ' copy both worksheets to a new workbook
    wb.Sheets(Array(ws1.Name, ws2.Name)).Copy
    ActiveWorkbook.SaveAs filename

    ActiveWorkbook.Close

    If counter1 = 1 Then
        ws1.Visible = xlSheetHidden
    End If
    If counter2 = 1 Then
        ws2.Visible = xlSheetHidden
    End If

End Sub

```

PROGRAMME DE GENERATION DES TEMPLATES

```
Private Sub Importbtn_Click()

    Dim FilePath As String
    Dim sourceWorkbook As Workbook
    Dim sourceWorksheet As Worksheet
    Dim targetWorksheet As Worksheet

    ' get the path to the external Excel file
    FilePath = Application.GetOpenFilename(fileFilter:="Excel Files (*.xlsx), *.xlsx")

    ' exit the subroutine if the user cancels the file selection
    If FilePath = "False" Then
        Exit Sub
    End If

    ' open the source workbook and set the source worksheet
    Set sourceWorkbook = Workbooks.Open(FilePath)
    Set sourceWorksheet = sourceWorkbook.Sheets("Sheet1")

    ' set the target worksheet in your current workbook
    Set targetWorksheet = ThisWorkbook.Sheets("Data Request List")

    ' copy the data from the source worksheet to the target worksheet
    sourceWorksheet.UsedRange.Copy
    targetWorksheet.Cells(1, 1).PasteSpecial xlPasteValuesAndNumberFormats

    ' close the source workbook without saving changes
    sourceWorkbook.Close SaveChanges:=False

End Sub
```

PROGRAMME D'IMPORTATION DES TEMPLATES REMPLIES

```

Private Sub Importbtn_Click()

    Dim riskProfileFilePath As String
    Dim riskProfileWorkbook As Workbook
    Dim riskProfileSheet As Worksheet

    Dim riskListSheet As Worksheet
    Dim riskListLastRow As Long
    Dim riskListRng As Range

    Dim profileRiskName As String
    Dim profileRiskPriority As String
    Dim profileRiskCat As String
    Dim profileRiskDesc As String
    Dim existingRiskRng As Range
    Dim existingRiskName As String

    ' Set the path to the risk profile file
    riskProfileFilePath = Application.GetOpenFilename("Excel files (*.xlsx), *.xlsm")
    If riskProfileFilePath = "False" Then
        MsgBox "No file selected."
        Exit Sub
    End If

    ' Open the risk profile workbook and sheet
    Set riskProfileWorkbook = Workbooks.Open(riskProfileFilePath)
    Set riskProfileSheet = riskProfileWorkbook.Sheets("RiskProfileTemplate")

    ' Set the RiskList sheet and range
    Set riskListSheet = ThisWorkbook.Sheets("RiskList")
    riskListLastRow = riskListSheet.Cells(Rows.Count, "A").End(xlUp).Row
    Set riskListRng = riskListSheet.Range("A2:C" & riskListLastRow)

    ' Loop through the rows of the risk profile sheet
    For i = 2 To riskProfileSheet.Cells(Rows.Count, "A").End(xlUp).Row

        ' Get the name and priority of the risk from the profile sheet
        profileRiskName = riskProfileSheet.Cells(i, 1).Value
        profileRiskPriority = riskProfileSheet.Cells(i, 6).Value
        profileRiskCat = riskProfileSheet.Cells(i, 3).Value
        profileRiskDesc = riskProfileSheet.Cells(i, 2).Value

        ' Check if the risk exists in the RiskList sheet
        Set existingRiskRng = riskListRng.Find(profileRiskName, LookIn:=xlValues)

        If Not existingRiskRng Is Nothing Then
            ' If the risk exists, update the priority
            existingRiskName = existingRiskRng.Value
            existingRiskPriority = riskListSheet.Cells(existingRiskRng.Row, 4).Value

            ' Define the priority order
            Select Case existingRiskPriority
                Case "Critical"
                    riskListSheet.Cells(existingRiskRng.Row, 4).Value = existingRiskPriority
                Case "High"
                    Select Case profileRiskPriority
                        Case "Critical"
                            If profileRiskPriority = "Critical" Then
                                riskListSheet.Cells(existingRiskRng.Row, 4).Value = profileRiskPriority

```

PROGRAMME DE CONSOLIDATION DES RISQUES (1/2)

```

' Define the priority order
Select Case existingRiskPriority
    Case "Critical"
        riskListSheet.Cells(existingRiskRng.Row, 4).Value = existingRiskPriority
    Case "High"
        Select Case profileRiskPriority
            Case "Critical"
                If profileRiskPriority = "Critical" Then
                    riskListSheet.Cells(existingRiskRng.Row, 4).Value = profileRiskPriority
                Else
                    riskListSheet.Cells(existingRiskRng.Row, 4).Value = existingRiskPriority
                End If
            End Select
    Case "Medium"
        If profileRiskPriority = "Critical" Then
            riskListSheet.Cells(existingRiskRng.Row, 4).Value = profileRiskPriority
        ElseIf profileRiskPriority = "High" Then
            riskListSheet.Cells(existingRiskRng.Row, 4).Value = profileRiskPriority
        Else
            riskListSheet.Cells(existingRiskRng.Row, 4).Value = existingRiskPriority
        End If
    Case "Low"
        If profileRiskPriority = "Critical" Then
            riskListSheet.Cells(existingRiskRng.Row, 4).Value = profileRiskPriority
        ElseIf profileRiskPriority = "High" Then
            riskListSheet.Cells(existingRiskRng.Row, 4).Value = profileRiskPriority
        ElseIf profileRiskPriority = "Medium" Then
            riskListSheet.Cells(existingRiskRng.Row, 4).Value = profileRiskPriority
        Else
            riskListSheet.Cells(existingRiskRng.Row, 4).Value = existingRiskPriority
        End If
    End Select
End Select

Debug.Print "Updated priority for risk: " & existingRiskName
Else
    ' If the risk doesn't exist, add a new row with the name and priority
    riskListSheet.Cells(riskListLastRow + 1, 1).Value = profileRiskName
    riskListSheet.Cells(riskListLastRow + 1, 4).Value = profileRiskPriority
    riskListSheet.Cells(riskListLastRow + 1, 2).Value = profileRiskCat
    riskListSheet.Cells(riskListLastRow + 1, 3).Value = profileRiskDesc
    Debug.Print "Added new risk: " & profileRiskName
    riskListLastRow = riskListLastRow + 1
End If
Next i

' Close the risk profile workbook
riskProfileWorkbook.Close False
Unload RiskForm
End Sub

```

PROGRAMME DE CONSOLIDATION DES RISQUES (2/2)

```

Private Sub Worksheet_Change(ByVal Target As Range)
Dim cell As Range
Dim hide As Boolean
Dim hide2 As Boolean
Dim hide3 As Boolean
Dim hide4 As Boolean
Dim Value_Old As String
Dim Value_New As String
If Target.Address = "$D$15" Then
    If Sheet6.Range("D15").Value = "No" Then
        hide4 = True
    ElseIf Sheet6.Range("D15").Value = "Yes" Then
        hide4 = False
    End If
    For Each cell In Sheets("Maturity Assessment").Range("B:B").Cells
        If cell.MergeCells And cell.Value = "OT Security" Then
            Sheets("Maturity Assessment").Rows(cell.MergeArea.Row & ":" & cell.MergeArea.Row + cell.MergeArea.Rows.Count - 1).EntireRow.Hidden = hide4
        End If
    Next cell
End If
If Target.Address = "$D$22" Then
    If Sheet6.Range("D22").Value = "No" Then
        hide = True
    ElseIf Sheet6.Range("D22").Value = "Yes" Then
        hide = False
    End If
    For Each cell In Sheets("Maturity Assessment").Range("B:B").Cells
        If cell.MergeCells And cell.Value = "Cloud Security" Then
            Sheets("Maturity Assessment").Rows(cell.MergeArea.Row & ":" & cell.MergeArea.Row + cell.MergeArea.Rows.Count - 1).EntireRow.Hidden = hide
        End If
    Next cell
End If
If Target.Address = "$D$26" Then
    Dim rngDropdown As Range
    Dim oldValue As String
    Dim newValue As String
    Dim DelimiterType As String
    DelimiterType = vbCrLf
    If Target.Count > 1 Then Exit Sub
    On Error Resume Next
    Set rngDropdown = Cells.SpecialCells(xlCellTypeAllValidation)
    On Error GoTo exitError
    If rngDropdown Is Nothing Then GoTo exitError
    If Intersect(Target, rngDropdown) Is Nothing Then
    Else
        Application.EnableEvents = False
        newValue = Target.Value
        Application.Undo
        oldValue = Target.Value
        Target.Value = newValue
        If oldValue <> "" Then
        If newValue <> "" Then

```

PROGRAMME DE PERSONNALISATION DES CONTROLES (1/2)

```

If rngDropdown Is Nothing Then GoTo exitError
If Intersect(Target, rngDropdown) Is Nothing Then
Else
    Application.EnableEvents = False
    newValue = Target.Value
    Application.Undo
    oldValue = Target.Value
    Target.Value = newValue
    If oldValue <> "" Then
        If newValue <> "" Then
            If oldValue = newValue Or
                InStr(1, oldValue, DelimiterType & newValue) Or
                InStr(1, oldValue, newValue & Replace(DelimiterType, " ", ""))
            Then
                Target.Value = oldValue
            Else
                Target.Value = oldValue & DelimiterType & newValue
            End If
        End If
    End If
End If
Dim searchWord As String

searchWord = "Intellectual property"
If InStr(1, Sheet6.Range("D26").Value, searchWord, vbTextCompare) > 0 Then
    hide2 = False
Else
    hide2 = True
End If
For Each cell In Sheets("Maturity Assessment").Range("B:B").Cells
    If cell.MergeCells And cell.Value = "Intellectual Property Security" Then
        Sheets("Maturity Assessment").Rows(cell.MergeArea.Row & ":" & cell.MergeArea.Row + cell.MergeArea.Rows.Count - 1).EntireRow.Hidden = hide2
    End If
Next cell
Dim searchWord2 As String

searchWord2 = "Protected Health Information"
If InStr(1, Sheet6.Range("D26").Value, searchWord2, vbTextCompare) > 0 Then
    hide3 = False
Else
    hide3 = True
End If
For Each cell In Sheets("Maturity Assessment").Range("B:B").Cells
    If cell.MergeCells And cell.Value = "Protected Health Information Security" Then
        Sheets("Maturity Assessment").Rows(cell.MergeArea.Row & ":" & cell.MergeArea.Row + cell.MergeArea.Rows.Count - 1).EntireRow.Hidden = hide3
    End If
Next cell

exitError:
    Application.EnableEvents = True
End If
End Sub

```

PROGRAMME DE PERSONNALISATION DES CONTROLES (2/2)

Bibliographie

- [1] High Value Manufacturing Catapult. Cyber Security Risk Assessment for Advanced Manufacturing.
- [2] CCA. <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>.
- [3] CIS. https://www.cisecurity.org/controls/v8_pre.
- [4] NIST CSF. <https://www.nist.gov/cyberframework>.
- [5] Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/about-deloitte-global-report-full-version-2022.pdf>.
- [6] Deloitte. <https://www2.deloitte.com/us/en/pages/risk/solutions/cyber-risk-services.html>.
- [7] Deloitte. <https://www2.deloitte.com/us/en/pages/mergers-and-acquisitions/articles/revenue-and-cost-synergy-diligence-in-mergers-and-acquisitions.html>.
- [8] Diligent. Five Steps to Implementing a Risk-Based Due Diligence Program.
- [9] Forbes. <https://www.forbes.com/sites/allbusiness/2020/04/17/impact-of-coronavirus-crisis-on-mergers-and-acquisitions/>.
- [10] Forescout. The Role of Cybersecurity in MA Due Diligence.
- [11] Gartner. Achieving MA Integration Requires Governance.
- [12] Gartner. Key IT Challenges in Mergers, Acquisitions and Divestments.
- [13] Gartner. Manage Operational Risk and Cybersecurity as a Business Service.
- [14] GDPR. <https://gdpr-info.eu/>.
- [15] HIPAA. <https://www.cdc.gov/phlp/publications/topic/hipaa.html>.

- [16] ISA. <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.
- [17] ISO. <https://www2.deloitte.com/us/en/pages/risk/solutions/cyber-risk-services.html>.
- [18] Alexandra Reed Lajoux and Charles M. Elson. The Art of MA Due Diligence.
- [19] Deloitte Consulting LLP. Technology Due Diligence Overview.
- [20] Mike Van Niekerk. VBA Automation for Excel 2019 Cookbook.
- [21] NIST. <https://csrc.nist.gov/News/2022/guide-to-operational-technology-ot-security>.
- [22] NIST. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>.
- [23] PCI. <https://www.pcisecuritystandards.org/>.
- [24] Mark Sirower and Jeff Weirens. The Synergy Solution : How Companies Win the Mergers and Acquisitions Game.
- [25] Mike Cisco. IT Due Diligence.