Une image contenant obscurité, noir, nuit, noir et blanc

Description générée automatiquement

Année universitaire : 2022-2023

Encadré par :

*Encadrant pédagogique :*

**M. AIT MADI Abdessalam**

*Maitres de stage :*

**Mme. IDRISSI Imane**

**M. AIT MBAREK Mohamed Amine**

Réalisé par :

**EL BAKKOURI Manal**

Effectué à :

**DELOITTE MOROCCO CYBER CENTER**

**CISO as a Service**

**RAPPORT DE PROJET DE FIN D’ETUDES**

**Filière : Réseaux et Systèmes de Télécommunications**

# **Dédicace**

*A mes chers parents*,

Les mots me manquent pour exprimer la profonde gratitude que j'éprouve envers vous, mon père et ma mère, pour votre amour inconditionnel, votre soutien permanent et vos encouragements tout au long de mon parcours. Depuis mes premiers pas jusqu'à cette réalisation majeure, vous avez été mon guide et ma source d'inspiration.

*Maman*, ta présence bienveillante et tes sacrifices incessants ont fait de moi la personne que je suis aujourd'hui. Ton amour infini et ta foi inébranlable en mes capacités ont alimenté ma détermination à surmonter les obstacles et à poursuivre mes rêves. Merci pour ton soutien permanent et pour avoir toujours été à mes côtés.

*Papa*, ta sagesse, tes conseils et ta foi inconditionnelle en mon potentiel ont été essentiels à ma réussite. Tes encouragements constants et ta recherche incessante de l'excellence m'ont inculqué les valeurs du travail acharné, de la persévérance et de l'intégrité. Je t'en serai éternellement reconnaissante.

*A Malak et Youssef*,

Je voudrais également dédier ce travail à ma chère sœur *Malak* et à mon adorable frère *Youssef.*

Malak, tu es bien plus qu'une sœur pour moi, tu es ma confidente et ma meilleure amie. Merci pour ton soutien inconditionnel et les moments précieux que nous partageons.

Youssef, tu es mon petit frère adoré, et même si tu es encore jeune, tu es une source constante de joie et de bonheur dans ma vie. Je suis honorée d'être votre sœur et je vous remercie d'enrichir ma vie de votre amour et de votre présence.

*A mes amis,*

En témoignage de la fraternité et l’attachement que je porte pour vous. Je ne vous remercierai jamais assez pour votre amabilité et générosité.

*Avec tout mon amour et ma gratitude,*

Manal

# **Remerciements**

Tout d'abord, je tiens à exprimer ma profonde gratitude à mon encadrant, M. AIT MADI Abdessalam, et ma Co encadrante Mme. Lalla Amina CHARAF, pour leurs précieux conseils, leurs avis éclairés et leur soutien constant tout au long de la réalisation de ce travail.

Mes sincères remerciements s'adressent également à Mme IDRISSI Imane et à M. AIT MBAREK MohamedAmine, mes superviseurs et encadrants au sein de l'entreprise, pour leur accueil chaleureux, leurs précieux conseils et leur patience. Leur disponibilité, leur expérience et leur expertise ont apporté une grande valeur ajoutée à mon projet et j'ai beaucoup appris à leur contact.

Je tiens également à exprimer ma gratitude à M. BERNOUSSI Marouan, Senior Manager de l'équipe Cyber, pour m'avoir donné l'opportunité de rejoindre cette équipe dynamique. Sa confiance en mes compétences et ses précieux conseils ont été une grande source d'inspiration pour moi.

Je tiens également à remercier M. EL ASRI Reda pour m'avoir donné l'opportunité d'effectuer ce stage. Sa confiance en mes capacités a été un facteur de motivation pour moi, et j'ai pu bénéficier d'une expérience professionnelle enrichissante.

Enfin, je tiens à exprimer ma profonde gratitude à M. EL KOURTBI Mohamed pour sa disponibilité et son suivi, et à toute l'équipe de Deloitte MCC pour leur soutien, leur expertise et leur esprit d'équipe qui ont été inestimables tout au long de ce stage. Leur collaboration et le partage de leurs connaissances ont contribué à mon développement professionnel et personnel.

Je tiens à remercier chaleureusement toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce rapport. Leur soutien, leurs conseils et leur engagement ont été essentiels à la réussite de ce projet.

Je suis profondément reconnaissante à chacun d'entre eux pour leur confiance, leurs conseils et leur contribution à ma réussite professionnelle.

# **Appreciation**

First, I would like to express my deep gratitude to my supervisor, Mr. AIT MADI Abdessalam, and my co-supervisor Ms. Lalla Amina CHARAF, for their invaluable advice, enlightened opinions, and constant support throughout the completion of this work.

My sincere thanks also go to Ms. IDRISSI Imane and Mr. AIT MBAREK Mohamed Amine, my supervisors at the company, for their warm welcome, invaluable advice and patience. Their availability, experience and expertise added great value to my project, and I learned a lot from them.

I would also like to express my gratitude to Mr. BERNOUSSI Marouan, Senior Manager of the Cyber team, for giving me the opportunity to join this dynamic team. His confidence in my skills and his invaluable advice were a great source of inspiration for me.

I would also like to thank Mr. EL ASRI Reda for giving me the opportunity to do this internship. His confidence in my abilities was a motivating factor for me, and I was able to benefit from an enriching professional experience.

Finally, I would like to express my deep gratitude to Mr. EL KOURTBI Mohamed for his availability and guidance, and to the entire Deloitte MCC team for their support, expertise, and team spirit, which have been invaluable throughout this internship. Their collaboration and sharing of knowledge contributed to my professional and personal development.

I would like to extend my warmest thanks to everyone who contributed in any way to the production of this report. Their support, advice and commitment were essential to the success of this project.

I am deeply grateful to each one of them for their trust, advice, and contribution to my professional success.

# **Table des matières**

[**Dédicace** 1](#_Toc136379432)

[**Remerciements** 2](#_Toc136379433)

[**Appreciation** 3](#_Toc136379434)

[**Table des matières** 4](#_Toc136379435)

[**Liste des tableaux** 10](#_Toc136379436)

[**Liste des acronymes** 11](#_Toc136379437)

[**Introduction générale** 12](#_Toc136379438)

[**Chapitre 1 : Présentation de l’entreprise d’accueil** 14](#_Toc136379439)

[**Introduction** 15](#_Toc136379440)

[**1.1.** **Fiche technique de l’entreprise** 15](#_Toc136379441)

[**1.2.** **Risk Advisory** 16](#_Toc136379442)

[**1.3.** **Deloitte Morocco Cyber Center - DMCC** 17](#_Toc136379443)

[**1.4.** **Pilier Principal** 18](#_Toc136379444)

[**1.5.** **Description du déroulement de stage** 19](#_Toc136379445)

[**Conclusion** 20](#_Toc136379446)

[**Chapitre 2 : Contexte général du Projet** 23](#_Toc136379447)

[**Introduction** 24](#_Toc136379448)

[**2.2. Cahier de charges** 26](#_Toc136379449)

[**2.3. Etude préalable** 26](#_Toc136379450)

[**2.4. Plan d’action** 29](#_Toc136379451)

[**2.5. Planning** 29](#_Toc136379452)

[**Conclusion** 31](#_Toc136379453)

[**Chapitre 3 : Etude détaillée du Projet** 33](#_Toc136379454)

[**Introduction** 34](#_Toc136379455)

[**3.1. Description de la solution** 34](#_Toc136379456)

[**3.2. Conception générale du Framework** 37](#_Toc136379457)

[3.2.1. Cas d’utilisation 37](#_Toc136379458)

[3.2.2. Normes et standards 38](#_Toc136379459)

[3.2.3. Aperçu du Framework 42](#_Toc136379460)

[**3.3. Services et catégories traités** 48](#_Toc136379461)

[3.3.1. Gouvernance 49](#_Toc136379462)

[3.3.2. Risk Management 50](#_Toc136379463)

[3.3.3. Conformité 50](#_Toc136379464)

[3.3.4. Sécurité opérationnelle 51](#_Toc136379465)

[3.3.5. Résilience 60](#_Toc136379466)

[3.3.6. Project Delivery Lifecycle : 60](#_Toc136379467)

[**Conclusion** 61](#_Toc136379468)

[**Chapitre 4 : Réalisation du Projet** 62](#_Toc136379469)

[**Introduction** 63](#_Toc136379470)

[**4.1.** **Contexte et objectif de la mission** 63](#_Toc136379471)

[**4.2.** **Méthodologie suivie pendant la mission** 64](#_Toc136379472)

[4.2.1. Planification 64](#_Toc136379473)

[4.2.2. Evaluation 64](#_Toc136379474)

[4.2.3. Recommandation et implémentation 70](#_Toc136379475)

[**Conclusion** 71](#_Toc136379476)

[**Conclusion générale** 72](#_Toc136379477)

[**Bibliographie** 74](#_Toc136379478)

[**Annexes** 76](#_Toc136379479)

[**Résumé** 78](#_Toc136379480)

[**Abstract** 79](#_Toc136379481)

# **Liste des figures**

[Figure 1.1: Chiffres d'affaires Deloitte durant les 3 dernières années 11](#_Toc136370875)

[Figure 1.2: Nombre de collaborateurs Deloitte durant les 3 dernières années 11](#_Toc136370876)

[Figure 1.3: Deloitte Morocco Cyber Center 13](#_Toc136370877)

[Figure 1.4: Services du DMCC 14](#_Toc136370878)

[Figure 2.1 : Les rôles du CISO 21](#_Toc136370879)

[Figure 2.2:Services CISO 23](#_Toc136370880)

[Figure 3.1: Approche proposée 31](#_Toc136370881)

[Figure 3.2: Cas d'utilisation de notre Framework 33](#_Toc136370882)

[Figure 3.3: Famille d'ISO 35](#_Toc136370883)

[Figure 3.4: Les principes de COBIT 38](#_Toc136370884)

[Figure 3.5: Aperçu feuille d’introduction 39](#_Toc136370885)

[Figure 3.6: Aperçu des cas d'utilisation 39](#_Toc136370886)

[Figure 3.7: Aperçu liste des catégories de chaque service 40](#_Toc136370887)

[Figure 3.8: Aperçu feuille Gouvernance 41](#_Toc136370888)

[Figure 3.9: Aperçu du mapping 43](#_Toc136370889)

[Figure 3.10: Niveau de scoring CMMI 43](#_Toc136370890)

[Figure 3.11: Matrice de scoring 44](#_Toc136370891)

[Figure 3.12: Catégories Gouvernance 45](#_Toc136370892)

[Figure 3.13: Catégories Risk Management 46](#_Toc136370893)

[Figure 3.14: Catégories Sécurité Opérationnelle 47](#_Toc136370894)

[Figure 3.15: Sous catégories prévention des menaces 47](#_Toc136370895)

[Figure 3.16: Sous-catégories détection des menaces 51](#_Toc136370896)

[Figure 4.1: Méthodologie suivie pendant la mission 60](#_Toc136370897)

[Figure 4.2: Assessment service Gouvernance 62](#_Toc136370898)

[Figure 4.3: Représentation du niveau de maturité 63](#_Toc136370899)

[Figure 4.4: Aperçu du niveau de maturité global sur le Dashboard 64](#_Toc136370900)

[Figure 4.5: Aperçu détaillé des services sur le Dashboard 64](#_Toc136370901)

[Figure 4.6: Aperçu détaillé des services sur le Dashboard 65](#_Toc136370902)

[Figure A.1: Programme VBA service G et RM 71](#_Toc136370903)

[Figure A.2: Programme VBA service Compliance 71](#_Toc136370904)

[Figure A.3: Programme VBA TP 72](#_Toc136370905)

[Figure A.4: Programme VBA Résilience 72](#_Toc136370906)

[Figure A.5: Programme VBA Dashboard 72](#_Toc136370907)

# **Liste des tableaux**

[Table 1: Services de Deloitte 6](#_Toc136267952)

[Table 2: Catégories de risques au sein de Risk Advisory 7](#_Toc136267953)

[Table 3: Planning stage 20](#_Toc136267954)

# **Liste des acronymes**

**CISO:** Chief Information Security Officer

**RSSI :** Responsable de ma Sécurité des Systèmes d'Information

**CISOaaS:** CISO as a Service

**SecOps:** Security Operations

**G:** Gouvernance

**RM:** Risk Management

**TP:** Threat Prevention

**TD :** Threat Detection

# **Introduction générale**

Ce rapport de stage PFE décrit mon expérience au sein de Deloitte Morocco Cyber Center, où j'ai effectué un stage portant sur le thème du CISO as a Service. Ce stage s'inscrit dans le cadre de ma formation académique et a été réalisé dans le but de développer un toolkit complet comprenant une approche et un Framework dédiés à la sécurité de l'information.

Le rapport est structuré en quatre chapitres, couvrant les différentes étapes de mon stage. Le premier chapitre est consacré à la présentation de mon entreprise d'accueil, Deloitte Morocco Cyber Center. Nous examinerons son positionnement sur le marché de la cybersécurité ainsi que ses domaines d'expertise.

Le deuxième chapitre traite le contexte général du projet. Nous discuterons des enjeux actuels de la sécurité de l'information et de la nécessité pour les organisations d'avoir une approche solide du CISO en tant que service. Nous mettrons en évidence les défis et les opportunités qui ont motivé le développement du toolkit, ainsi que les objectifs fixés pour sa conception.

Le troisième chapitre est consacré à une étude détaillée du projet. Nous décrirons en détail l'approche et le Framework développés, en nous concentrant sur les différentes phases de leur élaboration, les méthodologies utilisées et les principaux éléments qui les composent. Nous expliquerons également comment ces outils peuvent être appliqués dans un environnement réel pour améliorer la sécurité de l'information d'une organisation.

Enfin, le quatrième chapitre se concentre sur la mise en œuvre du projet. Nous présenterons les différentes étapes de la mise en œuvre du toolkit, en soulignant les résultats obtenus, les difficultés rencontrées et les enseignements tirés. Nous évoquerons également les perspectives et les recommandations pour l'amélioration continue du toolkit.

Ce rapport de stage a pour objectif de donner un aperçu de mon expérience au sein du Deloitte Morocco Cyber Center, ainsi que des résultats obtenus dans le cadre du projet de développement du toolkit CISO as a Service. Il représente une opportunité de partager les connaissances et l'apprentissage acquis durant cette période de stage, tout en mettant en avant les compétences techniques et professionnelles développées.

Il convient de noter que certaines informations spécifiques relatives à l'entreprise d'accueil et aux projets des clients ont été omises ou rendues anonymes afin de respecter les obligations de confidentialité. Toutefois, cela n'affecte en rien la compréhension globale du rapport ou la présentation des résultats obtenus.

Dans la suite de ce rapport, nous discutons chaque chapitre en détail, en soulignant les aspects clés du projet et en fournissant des analyses approfondies.

# **Chapitre 1 : Présentation de l’entreprise d’accueil**

## **Introduction**

Dans ce premier chapitre, nous introduisons l'organisme d'accueil, qui est l'entreprise prestataire du projet. Nous présentons brièvement la fiche technique de l'entreprise, en mettant en évidence des informations clés telles que son nom, son adresse et sa taille. Ensuite, nous abordons les domaines d'activité de l'entreprise, en soulignant les secteurs dans lesquels elle exerce ses activités principales. Enfin, nous donnons un aperçu de la structure et de l'organisation générale de l'entreprise, en mettant en avant les départements et les équipes qui la composent. Ces informations fournissent un contexte essentiel pour la suite de notre étude.

## **Fiche technique de l’entreprise**

Deloitte est un acteur mondial de référence en Audit et Conseil avec un héritage de plus de 175 ans d’excellence. Deloitte est réputée d’être le plus ancien et le plus large des cabinets BIG 4 avec un chiffre d’affaires qui s’est élevé à **59.3 milliards d’USD** en 2022, et une expertise de plus de **411.000** professionnels couvrant plus de **150** pays.

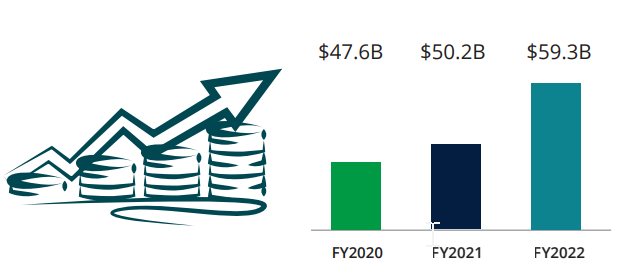


Figure 1.1: Chiffres d'affaires Deloitte durant les 3 dernières années

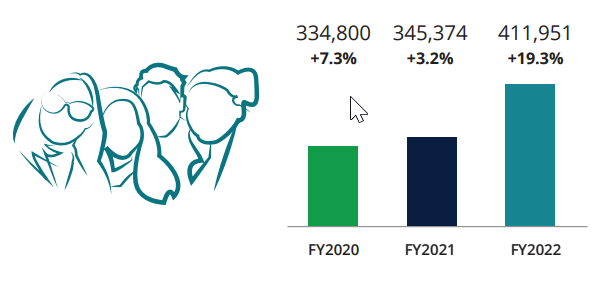


Figure 1.2: Nombre de collaborateurs Deloitte durant les 3 dernières années

Deloitte mobilise un ensemble de compétences diversifiées pour répondre aux enjeux de ses clients, de toutes tailles et de tous secteurs en visant la qualité la plus élevée en matière de prestation de services et de conseils professionnels sur différents métiers :

|  |  |
| --- | --- |
| 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 | Répondre aux demandes d’un paysage réglementaire complexe et changeant tout en restant flexible en allant jusqu’à l’externalisation. |
| Financial Advisory | 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. |
| Juridique | Aider les entreprises à maîtriser et piloter leurs opérations, leurs tiers, leurs données et leurs projets. |
| Fiscalité | Anticiper des Cyber menaces toujours plus probables avec une approche stratégique de vigilance et de résilience. |
| Risk Advisory | Deloitte accompagne ses clients à connaître les risques, de les évaluer, les modéliser, afin de prendre des décisions éclairées. |

Table 1.1: Services de Deloitte

## **Risk Advisory**

Image de marque, impact de l’entreprise sur l’environnement, mise en conformité face à un environnement réglementaire complexe, protection des actifs numériques, Deloitte accompagne ses clients dans la gestion de tous ces risques s’articulant autour de 5 grandes catégories :

|  |  |
| --- | --- |
| STRATEGIC RISK | Aider les entreprises à identifier et maitriser 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. |

Table 1.2: Catégories de risques au sein de Risk Advisory

## **Deloitte Morocco Cyber Center - 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 sur le continent Africain.

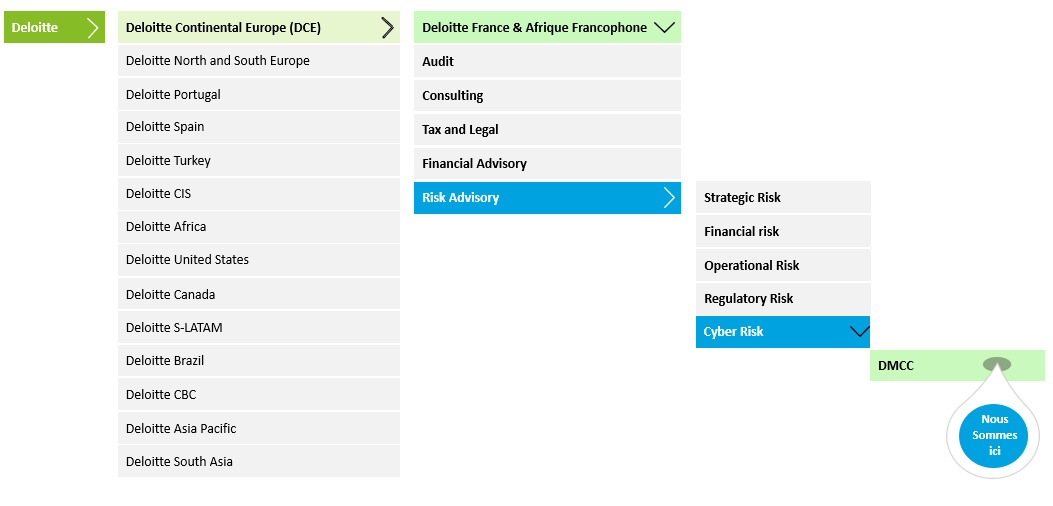


Figure 1.3: Deloitte Morocco Cyber Center

Le **DMCC** est le premier centre cyber en Afrique à offrir des services cyber en conformité avec les meilleures pratiques en matière de cybersécurité. Le centre se situe au cœur du **Casablanca Finance City**, la place économique et technologique connu comme le premier hub financier en Afrique.

Le **DMCC** vise à contribuer à favoriser l’emploi des experts et des ingénieurs Marocains diplômés des grandes écoles et universités d’ingénierie au Maroc en leur offrant le meilleur environnement de travail et l’opportunité de développer leurs compétences, et à développer un écosystème local en cybersécurité qui rayonnera au niveau national, régional et mondial.

Faisant partie d’un réseau de centre Deloitte de services cyber, avec un **mode opérationnel 24/7**, et un effectif de plus de **100 experts** dans le domaine, le centre **DMCC** fournit des services managés et un accompagnement rapproché à ses clients autour du globe sur les différents piliers couvrant l’ensemble des activités de la cybersécurité.

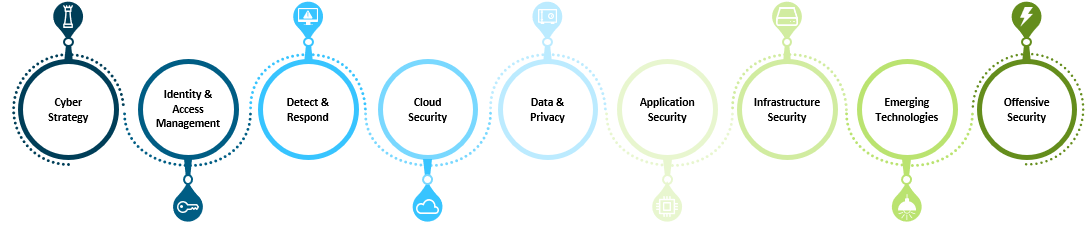


Figure 1.4: Services du DMCC

* **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 nos 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.

## **Pilier Principal**

Le pilier dans lequel j’ai effectué mon stage est le pilier Cyberstrat qui vise à aider les clients à aligner leur stratégie de cybersécurité idéale avec leurs objectifs stratégiques dans une ère où la cyber est omniprésente.

Dans un environnement où les menaces et les risques liés à la cybercriminalité sont de plus en plus présents, il est essentiel pour les entreprises de développer une stratégie de cybersécurité solide qui réponde à leurs besoins spécifiques et qui soit alignée sur leurs objectifs globaux.

Le pilier Cyberstrat se concentre sur cette dimension stratégique en travaillant étroitement avec les clients pour comprendre leurs objectifs, leurs défis et leurs priorités. Nous mettons en place des processus et des outils pour évaluer leur posture de cybersécurité actuelle, identifier les lacunes et les vulnérabilités, et formuler une stratégie sur mesure qui renforce leur résilience face aux cybermenaces.

Notre approche repose sur une analyse approfondie des risques, une compréhension des enjeux propres à chaque industrie et une expertise en matière de cybersécurité. Nous travaillons en étroite collaboration avec nos clients pour élaborer des recommandations concrètes et pragmatiques, en tenant compte de leurs ressources, de leur budget et de leurs contraintes opérationnelles.

L'objectif ultime du pilier Cyberstrat est d'aider nos clients à prendre des décisions éclairées et à mettre en place une stratégie de cybersécurité efficace qui protège leurs actifs numériques, leur réputation et leurs opérations. En les accompagnant dans ce processus, nous les aidons à naviguer dans cet environnement complexe et en constante évolution où la cyber est partout.

## **Description du déroulement de stage**

Le 6 février 2023, j'ai entamé mon stage au sein de Deloitte MCC. La première journée a été consacrée à l'intégration, au cours de laquelle notre senior manager et l'équipe des ressources humaines nous ont présenté l'organisation et les activités de Deloitte. Nous avons également eu un aperçu des différents piliers et de l'équipe. Par la suite, nous avons entamé les formations d'intégration ainsi que les formations sur les différentes plateformes d'e-learning.

Une semaine plus tard, j'ai été intégré à mon pilier principal, qui est le pilier Cyberstrat, et on m'a attribué mon sujet de stage. J'ai commencé par effectuer des recherches approfondies sur le sujet, ainsi que sur les normes et les standards internationaux qui me guideront dans l'élaboration de ma solution. Ensuite, j'ai défini l'approche à suivre et les différents services que je devais aborder pour ma solution. J'ai entamé la phase de conception de ma solution tout en suivant des formations complémentaires qui m'ont aidé dans cette démarche. De plus, j'ai régulièrement eu des points de suivi avec mon encadrant pour discuter de l'avancement du projet et recevoir des suggestions d'amélioration.

Par la suite, j'ai été intégré dans une mission client en lien avec mon sujet de stage, où j'ai pu constater concrètement l'utilité de ma solution et sa contribution à l'amélioration de la qualité du travail. Cette expérience m'a permis de mettre en pratique mes connaissances et de voir les résultats concrets de mes efforts.

Dans l'ensemble, mon stage chez Deloitte MCC a été une occasion unique de développer mes compétences, d'acquérir une expérience précieuse dans le domaine de la cybersécurité, et de voir comment mes efforts peuvent avoir un impact réel sur les clients et leur activité. Je suis reconnaissante d'avoir eu cette opportunité au sein d'une entreprise réputée telle que Deloitte.

## **Conclusion**

En conclusion, ce premier chapitre nous a permis de poser les bases de notre rapport de stage en présentant l'organisme d'accueil, l'équipe Cyber du service Risk Advisory et le pilier Cyberstrat auquel j'ai été rattaché. Nous avons également décrit le déroulement de ma période de stage, mettant en évidence les différentes étapes et activités auxquelles j'ai participé.

Ce chapitre a été essentiel pour contextualiser notre expérience de stage et fournir une compréhension claire de l'environnement dans lequel nous avons évolué. Il a permis de mettre en lumière l'importance de la cybersécurité et de la stratégie en matière de cybersécurité dans les entreprises actuelles, où les risques liés à la cybercriminalité sont omniprésents.

À travers notre intégration dans l'équipe Cyberstrat, nous avons pu développer nos connaissances et nos compétences dans le domaine de la cybersécurité, en nous familiarisant avec les normes et les meilleures pratiques internationales. Nous avons également eu l'occasion de mettre en pratique nos connaissances en participant à une mission client, où nous avons constaté l'impact concret de nos travaux sur l'amélioration de la sécurité et de la qualité du travail au sein de l'entreprise cliente.

Ce premier chapitre jette les bases pour les chapitres à venir, où nous approfondirons les détails de notre projet, les méthodologies utilisées, les résultats obtenus et les enseignements tirés de notre expérience de stage.

# **Chapitre 2 : Contexte général du Projet**

## **Introduction**

Dans ce chapitre, nous allons examiner comment les organisations peuvent bénéficier des avantages d'un CISO expérimenté et hautement qualifié pour garantir la sécurité de leurs systèmes et actifs, tout en minimisant les coûts et les complexités liées à cette fonction importante et nécessaire.   
**2.1. Description de la problématique**

La cybersécurité est une préoccupation majeure pour les organisations de toutes tailles et de tous secteurs d'activité. Avec la numérisation croissante des activités commerciales, de plus en plus d'informations et de données sensibles sont stockées sur des ordinateurs, des serveurs, des réseaux et des applications. Cette évolution a également conduit à l'émergence de nouvelles menaces telles que les attaques de logiciels malveillants, le phishing, l'usurpation d'identité, la fraude en ligne et bien d'autres.

La gestion de la cybersécurité d'une organisation nécessite une approche globale et proactive de la protection de ses actifs numériques et de ses informations confidentielles. Cela implique la mise en œuvre de mesures de sécurité techniques, organisationnelles et humaines pour prévenir, détecter et répondre aux menaces de cybersécurité.

Le CISO (Chief Information Security Officer) ou le RSSI (Responsable de la Sécurité des Systèmes d'Information) est le responsable de la cybersécurité au sein d'une organisation, son rôle est de superviser et d'assurer la sécurité des informations et des systèmes d'information d'une organisation. Il travaille en étroite collaboration avec d'autres cadres et dirigeants pour élaborer et mettre en œuvre des politiques et des procédures de sécurité visant à protéger les actifs de l'entreprise contre les menaces internes et externes.

Le CISO est également responsable de la gestion de la cybersécurité et de la technologie de l'entreprise, ce qui implique la mise en œuvre de mesures de sécurité pour protéger les réseaux, les serveurs, les données, les applications et les équipements de l'entreprise. Il est également chargé de veiller au respect des réglementations en matière de sécurité de l'information et de cybersécurité.

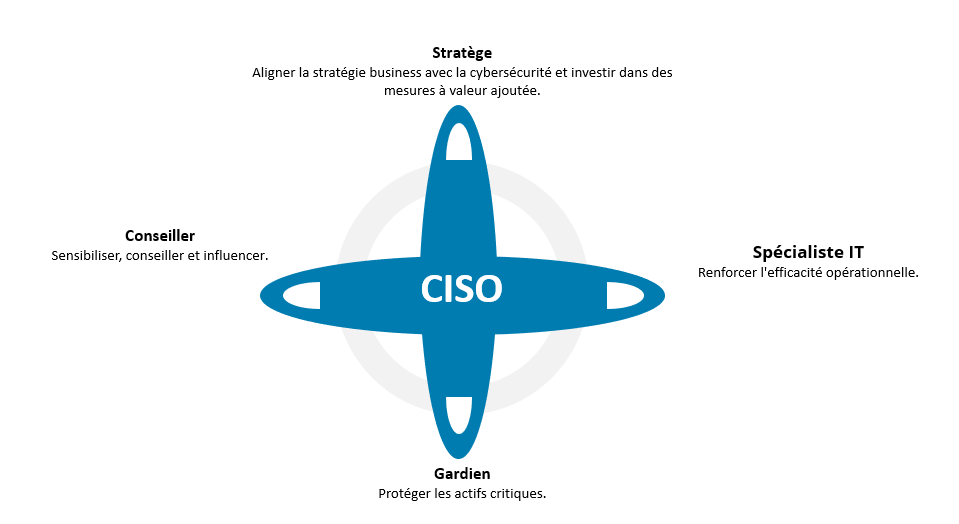


Figure 2.1 : Les rôles du CISO

Cependant, les organisations peuvent être confrontées à des difficultés pour couvrir les budgets et les ressources nécessaires à la fonction du CISO.

L'un des principaux défis est la concurrence pour les ressources et les budgets au sein de l'organisation, qui peut être exacerbée par la perception que la sécurité de l'information n'est pas une priorité. En outre, les coûts associés à la mise en œuvre des mesures de sécurité peuvent être élevés, ce qui peut constituer un obstacle pour les entreprises qui n'ont pas les moyens financiers de le faire.

Le recrutement et la fidélisation de spécialistes de la sécurité compétents et qualifiés pour ce poste peuvent constituer un autre défi pour les entreprises en raison de la pénurie de personnel qualifié dans le domaine de la sécurité de l'information. Enfin, la complexité croissante des menaces et des réglementations en matière de sécurité peut rendre difficile le maintien d'une sécurité de l'information adéquate, ce qui peut nécessiter des investissements importants en temps et en ressources pour le CISO et son équipe.

De ce fait **comment les organisations peuvent-elles bénéficier des avantages d'un CISO expérimenté et hautement qualifié pour garantir la sécurité de leurs systèmes et actifs, tout en minimisant les coûts et les complexités liées à cette fonction importante et nécessaire au sein de chaque organisation ?**

## **2.2. Cahier de charges**

La réponse à notre problématique est le "CISO as a Service" (CISOaaS), qui permettra aux entreprises de bénéficier des services d'un CISO expérimenté et hautement qualifié sans avoir à embaucher un CISO interne à temps plein.

Le CISOaaS est un modèle de prestation de services de sécurité de l'information dans lequel une organisation externalise la fonction de RSSI auprès d'un prestataire de services de sécurité de l'information spécialisé. En optant pour le modèle CISOaaS, les organisations peuvent bénéficier de l'expertise et des connaissances d'un CISO qualifié sans avoir à supporter les coûts liés à l'embauche et à la formation d'un CISO interne.

Le modèle CISOaaS peut également offrir des avantages tels que la flexibilité d'ajuster la couverture en fonction des besoins de l'entreprise, des économies par rapport à l'embauche d'un CISO interne à temps plein, et l'accès aux dernières technologies et aux meilleures pratiques en matière de sécurité de l'information.

Dans ce sens, l'objectif principal de mon stage est de définir, développer et mettre en œuvre une boîte à outils permettant de fortifier l’offre CISOaaS de Deloitte proposée à ses clients pour comprendre leurs besoins en matière de sécurité, élaborer une stratégie de sécurité sur mesure et mettre en œuvre des politiques, des procédures et des contrôles de sécurité efficaces.

## **2.3. Etude préalable**

Nous avons envisagé divers services CISO qui abordent différents aspects de la sécurité de l'information au sein de l'organisation. Chaque service est ensuite subdivisé en plusieurs catégories.

Voici une ventilation détaillée des services de notre Framework CISO ainsi qu’une description/objectif de chaque service :



Figure 2.2:Services CISO

**Gouvernance :**

Le service de gouvernance assure une gouvernance solide de la sécurité de l'information en établissant des structures, des processus et des mécanismes de contrôle efficaces. Son objectif est de prendre des décisions stratégiques éclairées, d'assurer la conformité aux normes de sécurité, de gérer les risques de manière proactive et de promouvoir une culture de sécurité. Il vise également à garantir une allocation adéquate des ressources, à assurer la responsabilité et la transparence, et à maintenir une supervision continue pour une sécurité de l'information optimale.

**Risk management :**

Le service de gestion des risques met en place des processus et des méthodologies pour identifier, évaluer et gérer les risques liés à la sécurité de l'information. Son objectif est de minimiser les impacts potentiels des risques en mettant en place des mesures de prévention, de mitigation et de réponse appropriées. Il vise à fournir une vision globale des risques, à promouvoir une culture de gestion des risques au sein de l'organisation et à garantir une prise de décision éclairée en matière de sécurité. Le service de gestion des risques travaille en étroite collaboration avec les parties prenantes internes et externes pour assurer une gestion proactive et efficace des risques liés à la sécurité de l'information.

**Conformité :**

Le service de conformité assure la conformité aux normes, réglementations et politiques en matière de sécurité de l'information. Son objectif est de garantir que l'organisation respecte les exigences légales et réglementaires pertinentes, ainsi que les normes et politiques internes établies. Le service de conformité évalue, surveille et rapporte la conformité, identifie les écarts et met en œuvre des mesures correctives. Il travaille en collaboration avec les différentes parties prenantes pour garantir la conformité continue et maintenir un niveau élevé de sécurité de l'information. Son rôle est essentiel pour réduire les risques juridiques et financiers liés à la non-conformité et renforcer la confiance des clients et des partenaires dans les pratiques de sécurité de l'organisation.

**Sécurité opérationnelle :**

Le service de sécurité opérationnelle est chargé d'assurer le bon fonctionnement et la protection des systèmes, réseaux et données de l'organisation. Son objectif principal est de prévenir, détecter et répondre aux incidents de sécurité, ainsi que de mettre en place des mesures de protection et des contrôles opérationnels appropriés. Le service de sécurité opérationnelle met en œuvre des stratégies de surveillance, de gestion des vulnérabilités, de gestion des incidents et de gestion des changements pour maintenir un environnement sécurisé. Il collabore étroitement avec les équipes techniques et les autres services de sécurité pour garantir la mise en œuvre efficace des mesures de sécurité opérationnelle. Son rôle est crucial pour assurer la disponibilité, l'intégrité et la confidentialité des ressources informatiques de l'organisation et pour atténuer les risques opérationnels liés à la sécurité de l'information.

**Résilience :**

Le service de résilience est chargé de renforcer la capacité de l'organisation à résister, à s'adapter et à se rétablir rapidement des incidents de sécurité et des perturbations opérationnelles. Son objectif principal est d'assurer la continuité des opérations, la disponibilité des services critiques et la récupération efficace après un incident. Le service de résilience met en place des plans d'urgence, des procédures de réponse aux incidents, des mécanismes de sauvegarde et de restauration, ainsi que des tests réguliers pour évaluer la capacité de l'organisation à faire face aux situations de crise. Il travaille en étroite collaboration avec les équipes techniques, les parties prenantes internes et externes pour identifier les scénarios de risques, élaborer des plans de résilience appropriés et assurer une communication efficace pendant les incidents. Son rôle essentiel est de minimiser les impacts des incidents sur l'organisation, de protéger sa réputation et d'assurer la reprise rapide des activités critiques.

**Project Delivery Lifecycle :**

Le cycle de vie de la livraison de projet est un service essentiel du projet CISO qui vise à garantir la mise en œuvre réussie des initiatives liées à la sécurité de l'information. Son objectif principal est de gérer efficacement toutes les phases du cycle de vie d'un projet, de la planification à l'exécution, en passant par la conception, le développement et le déploiement. Le service de cycle de vie de la livraison de projet met en place des processus et des méthodologies standardisés pour assurer la qualité, le respect des délais, la coordination des ressources et la communication entre les différentes parties prenantes. Il s'assure que les projets de sécurité sont alignés sur les objectifs stratégiques de l'organisation et qu'ils répondent aux normes et aux exigences réglementaires. Le service de cycle de vie de la livraison de projet supervise également la gestion des risques, la surveillance des performances et la gestion des changements tout au long du processus. Son rôle clé est d'assurer la livraison réussie des projets de sécurité, en veillant à ce qu'ils soient livrés dans les délais, dans le respect du budget et conformément aux attentes de qualité.

## **2.4. Plan d’action**

Pour la concrétisation de notre solution, nous avons procédé comme suit :

* Familiarisation avec les différentes normes et standards internationaux
* Réalisation de l’approche
* Définition des services à traiter dans le cadre de notre projet
* Réalisation du Framework
* Réalisation des livrables attendus

## **2.5. Planning**

Pour assurer l'efficacité de notre travail, nous avons planifié des points réguliers par semaine avec mon encadrant de stage M. Mohamed Amine Ait Mbarek pour valider mes progrès et discuter des tâches à suivre.

De plus, nous avons planifié plusieurs points avec le manager de l'équipe Cyber Stratégie M. Mohamed El Kourtbi et la consultante sénior de l'équipe Cyber Stratégie Mme Imane Idrissi pour l'évaluation de notre avancement sur le stage. Ci-dessous se trouve le planning détaillé de l'ensemble de mon stage.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Phases du projet** | Février | | | | Mars | | | | Avril | | | | Mai | | | | | Juin | | | |
| 6 | 13 | 20 | 27 | 6 | 13 | 20 | 27 | 3 | 10 | 17 | 24 | 1 | 8 | 15 | 22 | 29 | 5 | 12 | 19 | 26 |
| **Phase 1 :** Intégration et formations |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Formation d’intégration Deloitte |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Formations cybersécurité sur les plateformes digitales Deloitte |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| **Phase 2 :** Contexte et planification |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Compréhension du contexte |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Etat d’art du projet |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| **Phase 3 :** Documentation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| ISO 27001 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Loi 05.20 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| ISO 27002 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| NIST SP800-53 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| **Phase 4 :** Réalisation du toolkit |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Version draft de l’approche |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Définition des services |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Définition des catégories et sous catégories |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Définition des contrôles, description et questions |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Définition des use cases |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Mapping vers les normes et Framework |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| **Phase 5 :** Mission client |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Phase de planification |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Phase d’évaluation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| Phase de recommandation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |

Table 2.1: Planning stage

## **Conclusion**

En conclusion, la sécurité de l'information est un enjeu critique pour toutes les organisations, mais il peut être difficile de trouver l'expertise nécessaire tout en gérant les coûts et les complexités. C'est pourquoi le CISO en tant que service peut être une solution intéressante pour les organisations qui cherchent à bénéficier des avantages d'un CISO hautement qualifié sans les coûts et les tracas de l'embauche en interne. Avec cette solution, les organisations peuvent accéder à une expertise spécialisée en matière de sécurité de l'information, des technologies de pointe et des bonnes pratiques de l'industrie. Cela permet aux organisations de se concentrer sur leur cœur de métier tout en bénéficiant d'un niveau élevé de protection pour leurs systèmes et leurs actifs. En considérant les avantages du CISO en tant que service, les organisations peuvent prendre une décision éclairée sur la meilleure façon de protéger leur entreprise contre les menaces internes et externes.

# **Chapitre 3 : Etude détaillée du Projet**

## **Introduction**

Ce chapitre explore le concept novateur du CISO as a Service, qui offre aux organisations la possibilité de bénéficier des services d'un CISO et d'une équipe de sécurité hautement qualifiée, sans les coûts et les contraintes liés à l'embauche d'un personnel interne dédié. Ce modèle permet aux entreprises de tirer parti de l'expertise et de l'expérience d'un CISO externe pour mettre en œuvre des stratégies de sécurité solides, évaluer les risques, garantir la conformité réglementaire et réagir de manière proactive aux menaces émergentes.

Au cours de ce chapitre, nous allons explorer en détail les six services clés qui composent notre modèle CISO as a Service. Chacun de ces services joue un rôle essentiel dans la protection des informations sensibles de l'organisation et dans la mise en place d'une culture de sécurité robuste. Nous examinerons les objectifs, les domaines d'intervention et les sous-catégories de chaque service, en mettant l'accent sur les meilleures pratiques et les stratégies éprouvées pour assurer la sécurité de l'information.

En comprenant ces services clés et en explorant leur mise en œuvre, vous serez en mesure de développer une vision complète du rôle du CISO as a Service.

## **3.1. Description de la solution**

La solution CISO as a Service consiste à externaliser la fonction de sécurité de l'information auprès d'un prestataire de services qualifié et expérimenté. Ce prestataire de services offre une expertise spécialisée en matière de sécurité de l'information, des technologies de pointe et les meilleures pratiques de l'industrie. Cette solution est particulièrement intéressante pour les organisations qui disposent de ressources limitées ou qui souhaitent se concentrer sur leur cœur de métier tout en bénéficiant d'un niveau élevé de protection de leurs systèmes et de leurs actifs.

Dans le cadre de cette mise en œuvre de la solution, Deloitte souhaite développer un toolkit qui aidera le CISO à gérer efficacement la sécurité de l'information. Ce toolkit comprendra une approche et un Framework afin de pouvoir élaborer une stratégie efficace en matière de sécurité de l'information, gérer les risques de manière proactive, surveiller les menaces et garantir la conformité aux réglementations.

Nous avons développé une approche en quatre phases pour répondre à ces besoins :

* La phase de planification consiste à analyser le contexte et les objectifs de sécurité de l'information, à déterminer le périmètre, le budget et les ressources nécessaires, à identifier les parties prenantes impliquées, à définir les rôles et responsabilités, et à élaborer un plan de projet.
* La phase d'évaluation de la maturité de la cybersécurité vise à analyser les contrôles de sécurité mis en place, à évaluer le corpus documentaire de sécurité de l'information, et à vérifier la conformité réglementaire.
* La phase de recommandation consiste à proposer des actions à entreprendre en fonction du niveau de maturité obtenu, afin d'améliorer les processus de sécurité de l'entreprise.
* Enfin, la phase d'implémentation se concentre sur la mise en œuvre des mesures de sécurité recommandées pour renforcer la protection des informations et garantir la conformité aux normes et réglementations en vigueur.

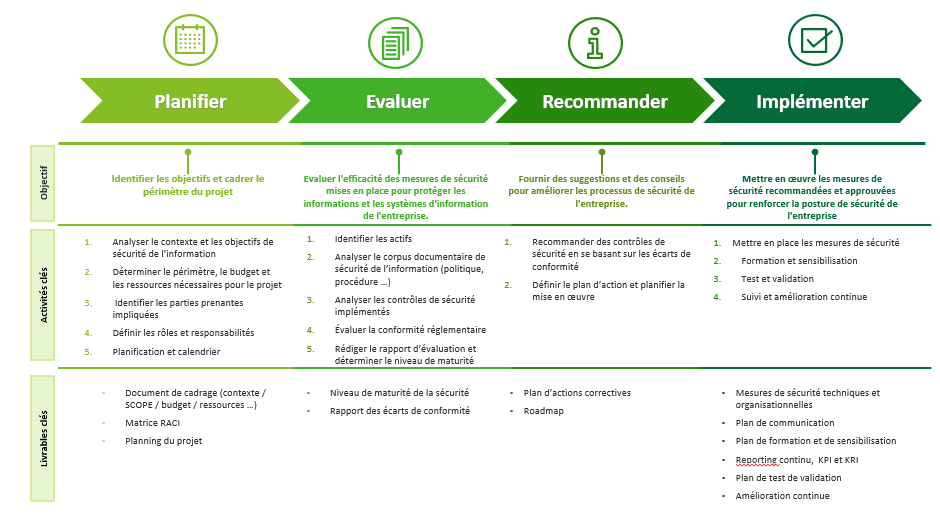


Figure 3.1: Approche proposée

A partir de cette approche, nous avons déployer notre Framework qui est conçu pour aider les organisations à évaluer leur niveau de maturité en matière de sécurité de l'information et à mettre en œuvre les contrôles nécessaires pour renforcer leur sécurité.

Il se compose d’une série de questions qui évaluent l'état actuel de la sécurité de l'organisation, ainsi que des normes pour évaluer la maturité de l'organisation dans plusieurs domaines clés de la sécurité de l'information. Une fois l'évaluation terminée, le Framework fournit des recommandations sur les contrôles à mettre en place pour renforcer la sécurité de l'organisation, en fonction de ses besoins et de ses objectifs.

Ce Framework peut être utilisé pour évaluer les processus, les politiques et les technologies de l'organisation et identifier les domaines dans lesquels des améliorations sont nécessaires. Les résultats de l'évaluation sont ensuite utilisés pour élaborer un plan d'action détaillé visant à mettre en œuvre les contrôles nécessaires pour renforcer la sécurité de l'organisation. Le Framework fournit également des recommandations sur les bonnes pratiques et politiques de sécurité de l'information afin de renforcer la culture de la sécurité de l'information au sein de l'organisation.

En utilisant ce Framework, les organisations peuvent améliorer de manière proactive leur position en matière de sécurité de l'information et s'assurer qu'elles répondent aux exigences de conformité et aux normes de l'industrie.

## **3.2. Conception générale du Framework**

### **3.2.1. Cas d’utilisation**

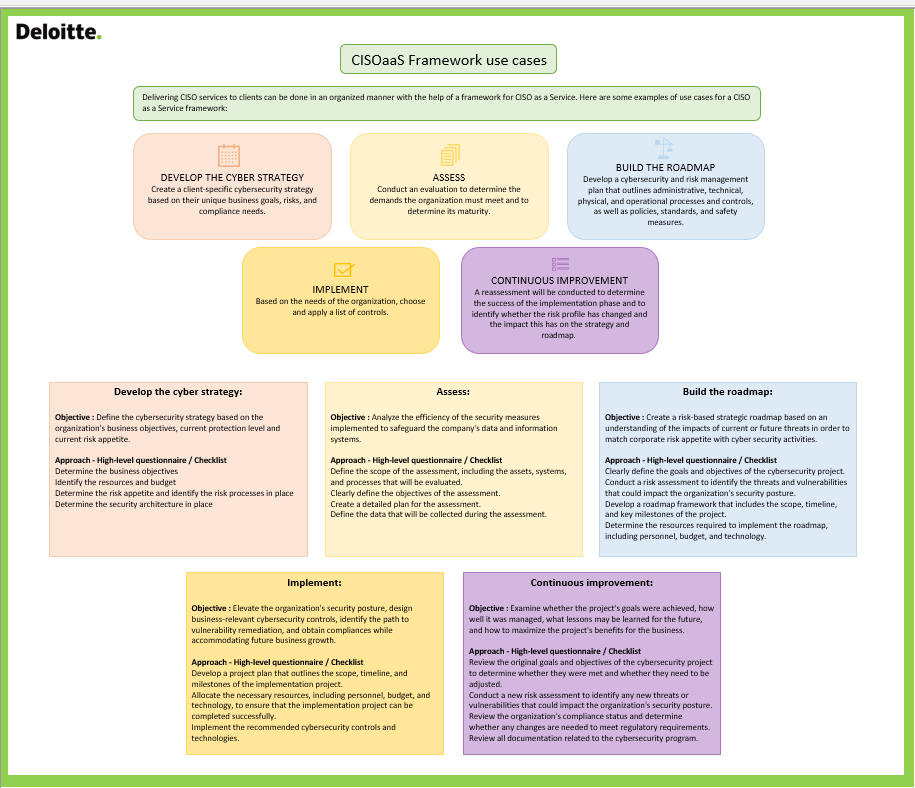


Figure 3.2: Cas d'utilisation de notre Framework

Lors de la conception de notre Framework CISOaaS, nous avons suivi une approche permettant de développer un outil couteau suisse pour différentes utilisations et use cases, et qui sont les suivants :

* Élaboration de la stratégie de cybersécurité : Nous élaborons une stratégie de cybersécurité spécifique à chaque client, en prenant en compte leurs objectifs commerciaux, leurs risques et leurs exigences en matière de conformité.
* Évaluation : Nous réalisons une évaluation pour déterminer les exigences auxquelles l'organisation doit répondre et évaluer son niveau de maturité en matière de cybersécurité.
* Définition de la feuille de route : Nous élaborons un plan de cybersécurité et de gestion des risques qui décrit les processus, les contrôles administratifs, techniques, physiques et opérationnels, ainsi que les politiques, les normes et les mesures de sécurité.
* Mise en œuvre : En fonction des besoins de l'organisation, nous sélectionnons et mettons en place une liste de contrôles appropriés.
* Amélioration continue : Nous effectuons une réévaluation pour évaluer le succès de la phase de mise en œuvre, identifier tout changement dans le profil de risque et déterminer son impact sur la stratégie et la feuille de route.

En concevant notre Framework CISOaaS, nous avons suivi une approche méthodique pour ces différentes étapes, visant à fournir à nos clients une stratégie de cybersécurité personnalisée, des mesures de contrôle adaptées et une amélioration continue de leurs pratiques de sécurité.

### **3.2.2. Normes et standards**

Pour développer notre Framework, nous nous sommes appuyés sur une variété de standards et de normes pour définir les contrôles et les aspects à prendre en compte, notamment :

#### **ISO 27001 / 27002**

La suite ISO/CEI 27000 (aussi connue sous le nom de Famille des standards SMSI ou ISO27k) comprend les normes de sécurité de l’information publiées conjointement par l'ISO et la Commission électrotechnique internationale (CEI, ou IEC en anglais). [2] La suite contient des recommandations des meilleures pratiques en management de la sécurité de l'information, pour l'initialisation, l'implémentation ou le maintien de systèmes de management de la sécurité de l'information. Ci-dessus, les différentes familles ISO 27000 avec leurs objectifs.

A picture containing text, screenshot, circle, font

Description automatically generated

Figure 3.3: Famille d'ISO

Cependant, on va se focaliser dans notre recherche sur la norme ISO 27001 et ses bonnes pratiques détaillées dans ISO27002. Ci-dessous un tableau résumant tous les thématiques de sécurité existantes dans ISO 27002.

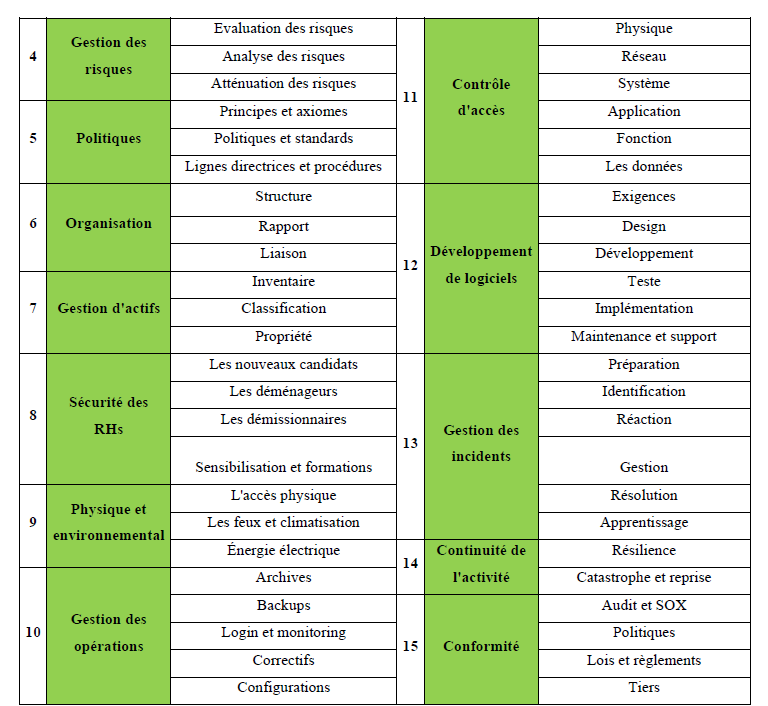


Tableau 3.1: Domaines de l'ISO 27002

#### **NIST SP 800-53**

Le but de NIST est de promouvoir l'économie en développant des technologies et des standards de l'industrie. Elle offre non seulement différents guides et méthodologies mais aussi un ensemble de recommandations et bonnes pratiques sur divers domaines d’industrie.

Plusieurs séries sont développées par NIST dans des domaines différents. On prend en compte la série NIST SP 800. Les publications SP 800 sont développées pour répondre et prendre en charge les besoins de sécurité et de confidentialité des systèmes d'information et d'information du gouvernement fédéral américain.

La publication NIST SP 800-53 fournit un catalogue de contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations afin de protéger les opérations et les actifs de l'organisation, les individus, les autres organisations et la Nation contre un ensemble diversifié de menaces et de risques.

Les familles de contrôles dans cette publication sont les suivants :

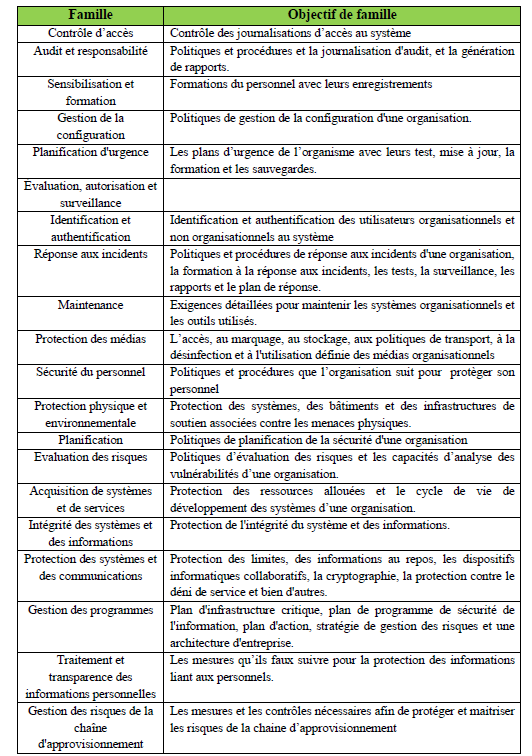


Tableau 3.1: Domaine de NIST SP 800-53

#### **COBIT v5**

COBIT (Control Objectives for Information and Related Technology) est un cadre de contrôles de gouvernance IT aidant les entreprises à faire face aux enjeux commerciaux dans les domaines de la conformité règlementaire, de la gestion des risques et de l’alignement de la stratégie IT avec des objectifs organisationnels.

Si dessus les 5 principes du référentiel COBIT.

A picture containing text, screenshot, circle, font

Description automatically generated

Figure 3.4: Les principes de COBIT

### **3.2.3. Aperçu du Framework**

Notre Framework est structuré en plusieurs feuilles pour faciliter sa compréhension et son utilisation :

* **Feuille d'introduction :** Cette feuille présente une vue d'ensemble du Framework et met en évidence les différents services qui seront abordés dans la suite du document. Elle permet aux utilisateurs de se familiariser avec les principaux aspects du Framework.

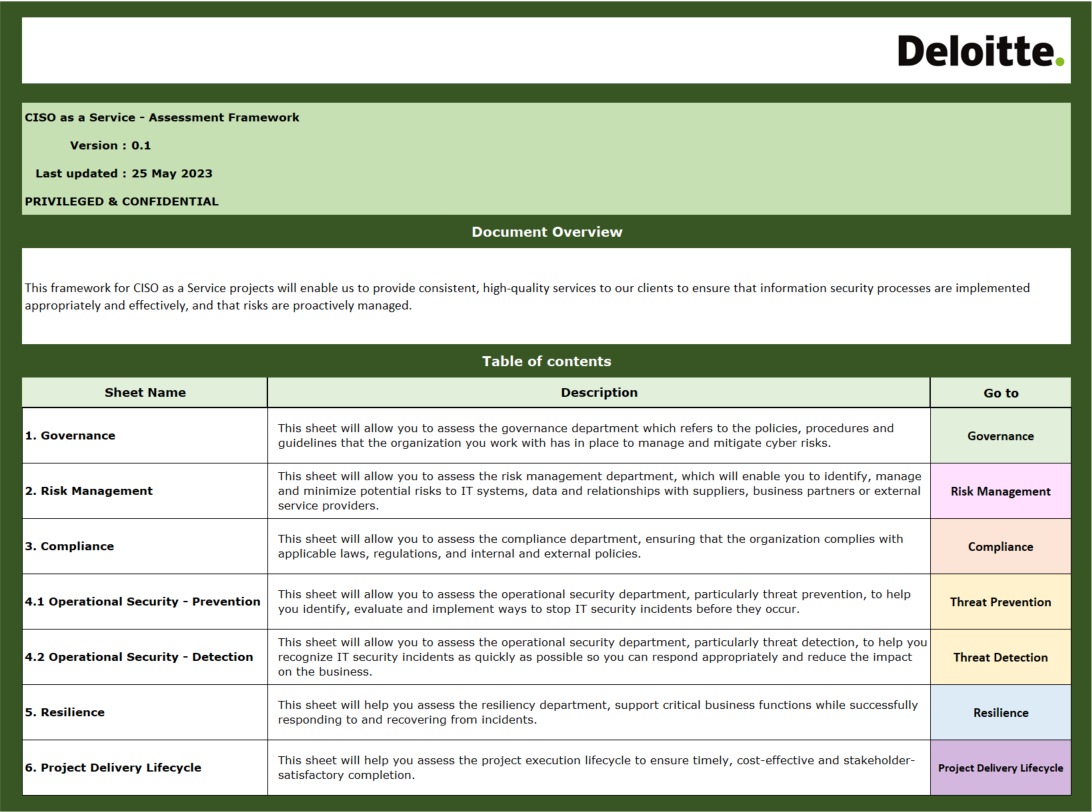


Figure 3.5: Aperçu feuille d’introduction

* **Feuille des cas d'utilisation** : Cette feuille détaille les différents cas d'utilisation de notre Framework. Elle fournit des informations spécifiques sur la manière dont le Framework peut être appliqué dans des situations concrètes. Cela permet aux utilisateurs de comprendre comment ils peuvent tirer parti du Framework en fonction de leurs besoins et de leurs objectifs.

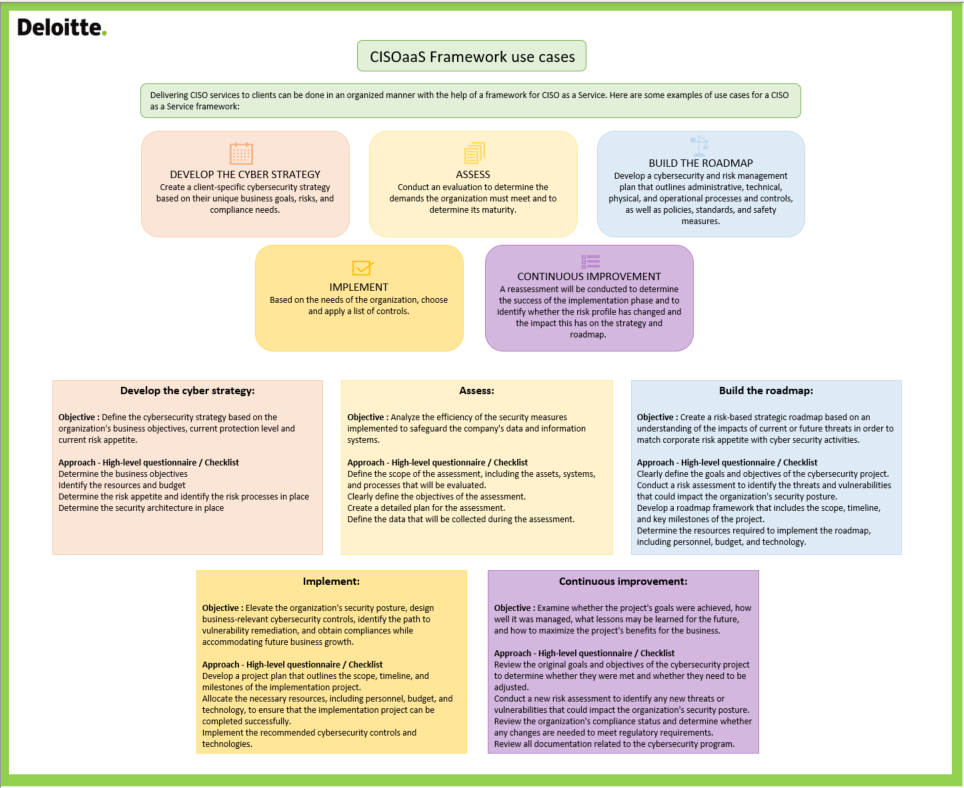


Figure 3.6: Aperçu des cas d'utilisation

* **Feuille des catégories et sous-catégories :** Cette feuille présente de manière claire et organisée les différentes catégories de services couvertes par notre Framework.

Chaque catégorie est accompagnée de ses sous-catégories correspondantes. Cette feuille permet aux utilisateurs de naviguer facilement à travers les différentes sections du Framework et de se concentrer sur les domaines qui les intéressent particulièrement.

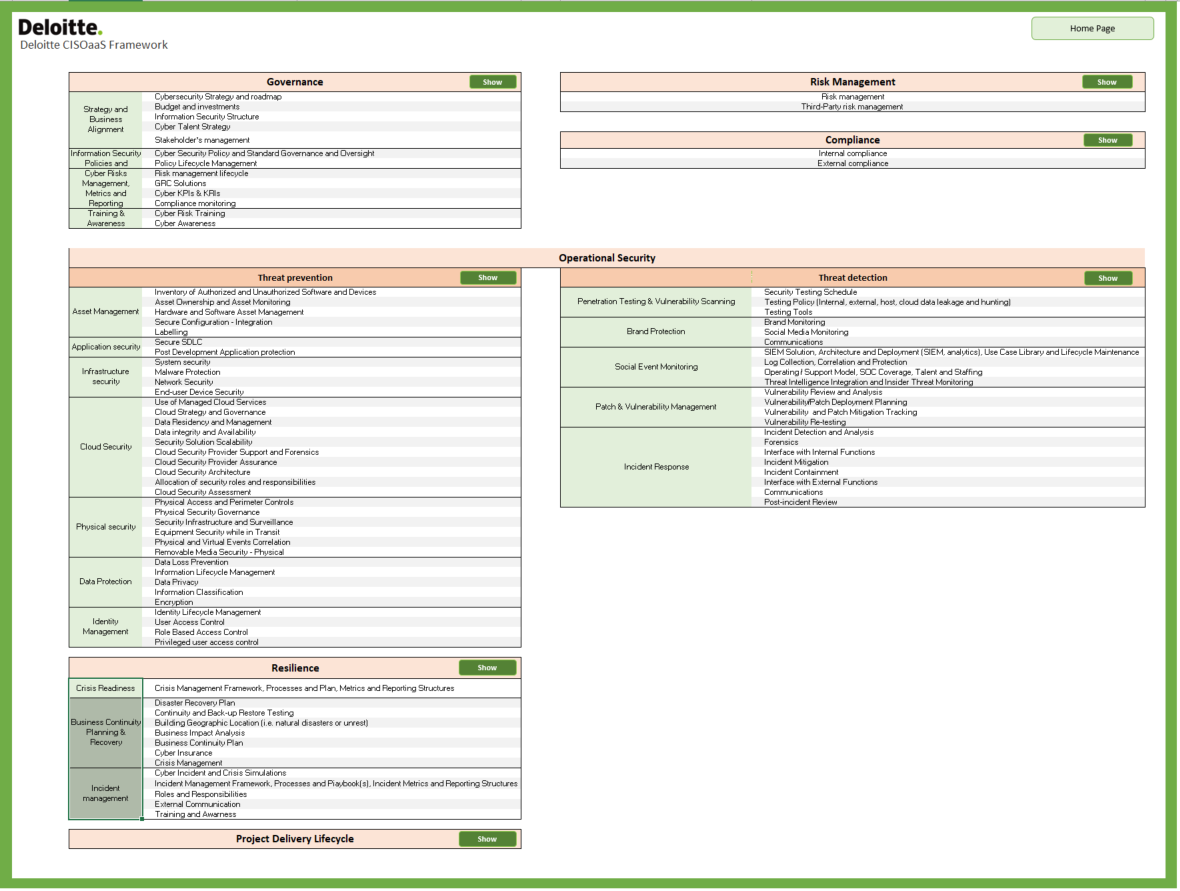


Figure 3.7: Aperçu liste des catégories de chaque service

En structurant notre Framework de cette manière, nous visons à fournir une organisation claire et logique de l'information, facilitant ainsi l'utilisation et la compréhension du document. Les différentes feuilles permettent aux utilisateurs de trouver rapidement les informations pertinentes et de se concentrer sur les aspects qui les concernent le plus.

* **Les feuilles principales :** Dans ces feuilles-là, nous traitons individuellement chaque service d’une manière approfondie et ceci de sorte que nous répondons aux différents cas d’utilisation auxquels nous avons pensé. Dans la capture ci-dessous je vous présenterai la feuille du service de la gouvernance.



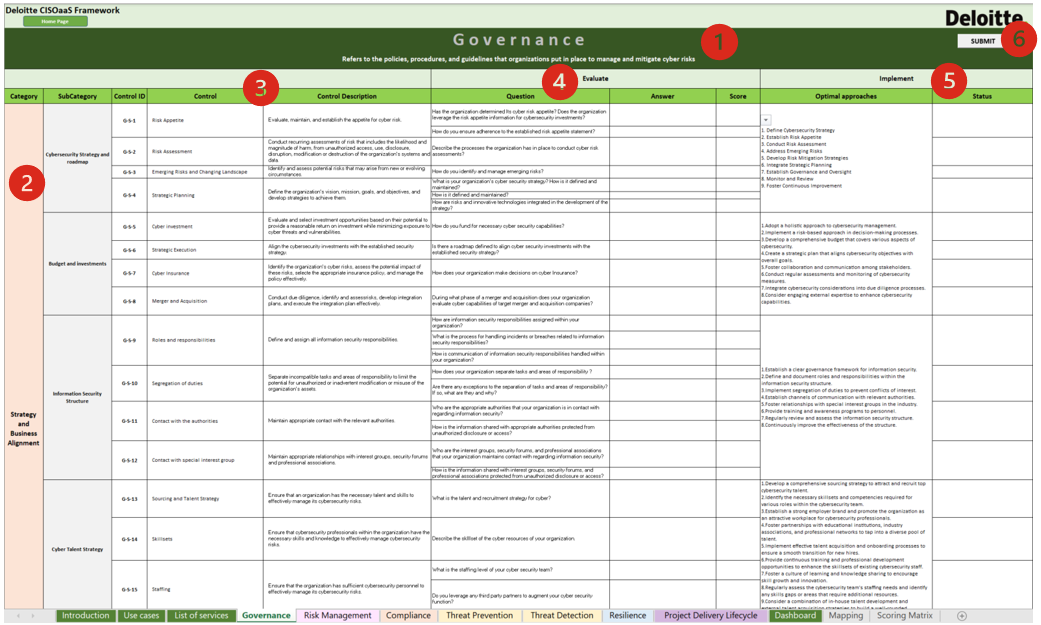


Figure 3.8: Aperçu feuille Gouvernance

 : ceci est une petite présentation du service actuel.



 : dans cette partie, nous avons les catégories suivies de leurs sous-catégories.

 : ce numéro fait référence aux différents contrôles sur lesquels notre travail va être basé, nous avons donné à chaque contrôle son propre ID, ainsi qu’une petite description.

 : cette partie là fait référence au deuxième cas d’utilisation que nous avons abordé, dont le principal objectif est d’évaluer le niveau de maturité de l’entreprise. Nous trouvons d’abord des questions relatives à chaque contrôle, suivies par un champ pour répondre et un autre pour assigner le score éloquent de 0 à 5.

 : pour le cas d’utilisation suivant relatif à l’implémentation, nous avons pensé à proposer les meilleures actions à entreprendre pour implémenter chaque sous catégories, suivi par une colonne qui va nous permettre de faire le suivi de l’implémentation des solutions proposées à partir du score obtenu préalablement.

 : finalement, ceci est un bouton programmé en VBA, qui simplifie la vérification des scores dans la base de données. Ce bouton nous permettra de suivre facilement le nombre de questions répondues et non répondues, tout en affectant automatiquement un score de 0 aux questions non répondues.

Grâce à ce code VBA ingénieux, une fois que vous cliquez sur le bouton, il effectuera les actions suivantes :

* Vérification de la case du score : Le bouton vérifiera si la case du score est remplie pour chaque question de la base de données.
* Comptage des questions répondues et non répondues : Il comptera le nombre de questions pour lesquelles un score a été saisi et les questions sans score.
* Attribution d'un score de 0 : Pour les questions non répondues, le bouton assignera automatiquement un score de 0 dans la base de données.

Grâce à cette fonctionnalité, nous pourrons rapidement identifier les questions non répondues et les associer à un score de 0, nous permettant ainsi d'avoir une vue d'ensemble précise de l'état de nos réponses.

Dans notre Framework, nous avons pris en compte l'ajout d'annexes pour renforcer son utilité. La première annexe vise à associer les contrôles aux normes et aux standards utilisés dans le développement des contrôles et des questions essentielles pour l'évaluation. Cela permet d'assurer que les contrôles mis en place sont conformes aux meilleures pratiques de l'industrie.

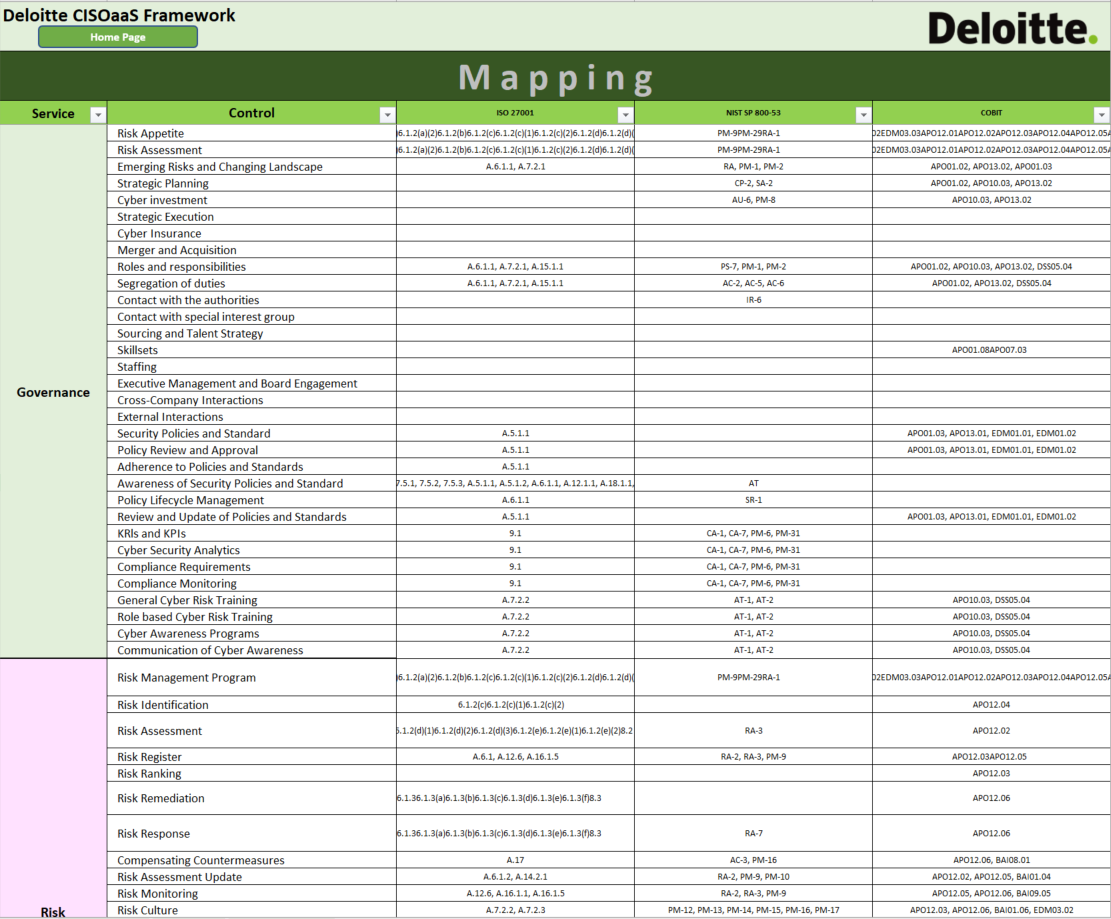


Figure 3.9: Aperçu du mapping

La deuxième annexe consiste en une matrice de scoring détaillant les niveaux de scoring, basée sur un système de scoring CMMI (Capability Maturity Model Integration) de 0 à 5.

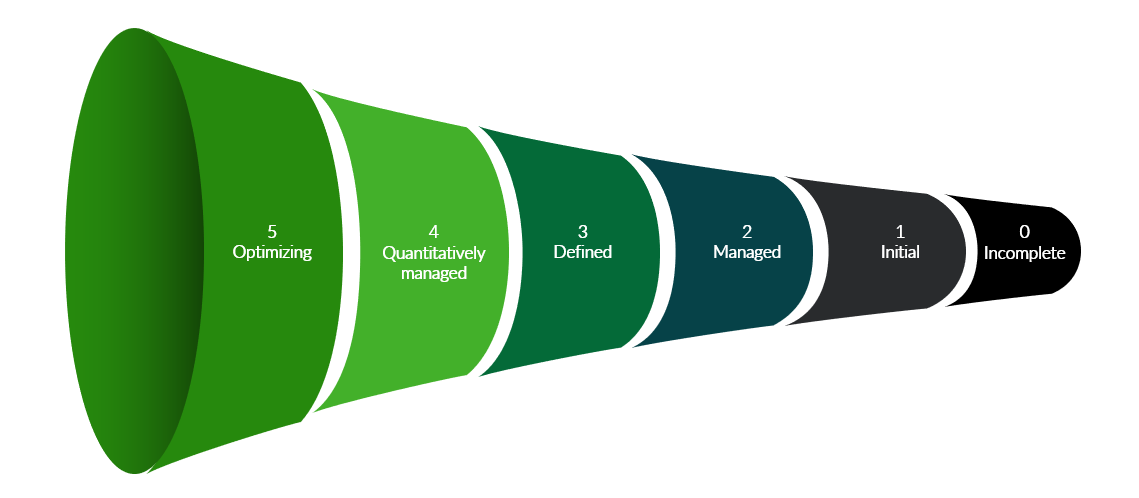


Figure 3.10: Niveau de scoring CMMI

Cette matrice fournit une évaluation quantitative de la maturité de la cybersécurité de l'organisation, en attribuant des scores aux différents domaines évalués. Elle permet de mesurer et de communiquer clairement le niveau de sécurité atteint par l'organisation, offrant ainsi une base solide pour l'amélioration continue des pratiques de cybersécurité.

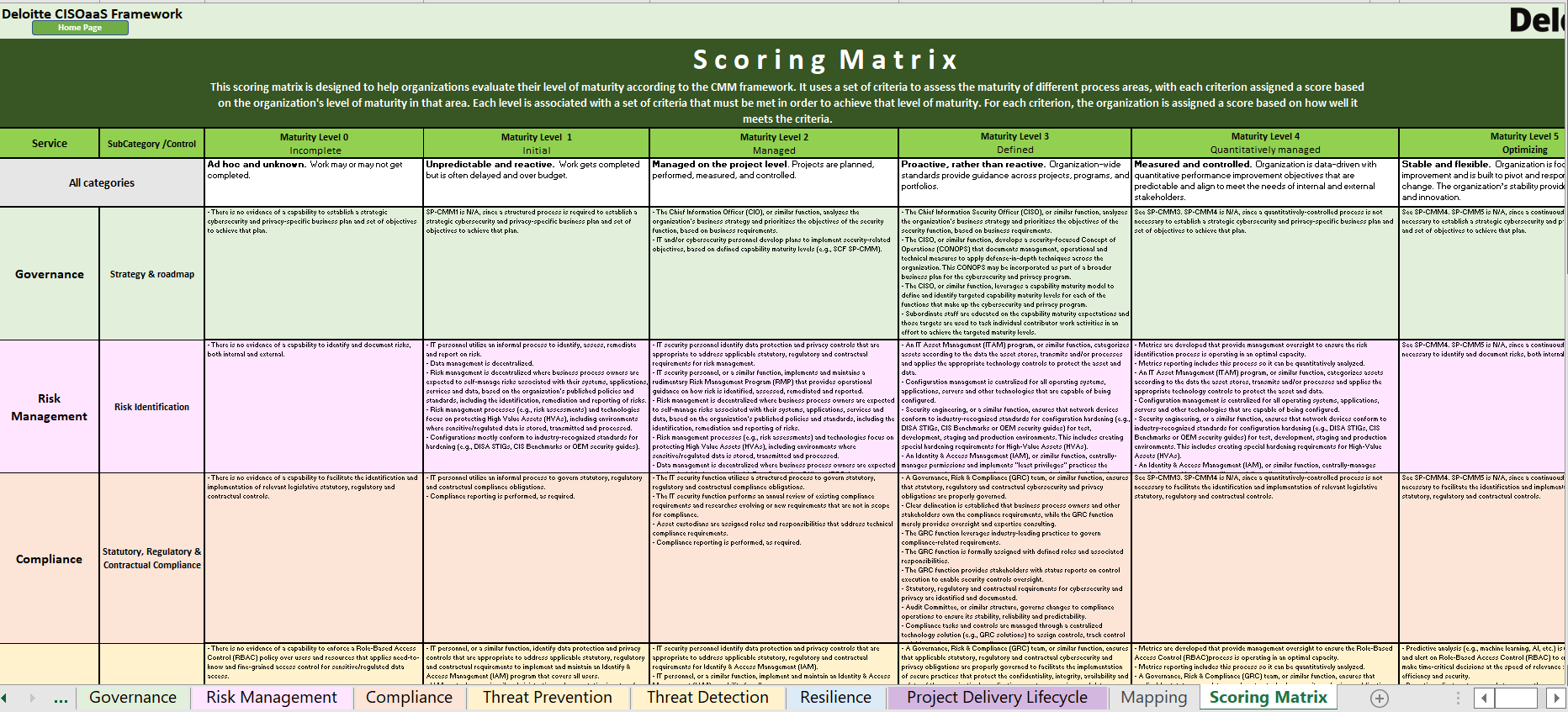


Figure 3.11: Matrice de scoring

En intégrant ces annexes dans notre Framework, nous visons à fournir des outils supplémentaires aux utilisateurs pour une évaluation approfondie de leur posture en matière de cybersécurité et pour les guider dans leur progression vers des niveaux de maturité plus élevés. Cela renforce l'efficacité et la pertinence de notre Framework, en fournissant des informations complémentaires et en permettant une évaluation plus précise de la cybersécurité.

## **3.3. Services et catégories traités**

Dans cette section du chapitre, nous allons examiner de manière détaillée les différentes catégories et sous-catégories de chaque service, en fournissant une explication claire de chacun d'entre eux et en mettant en évidence leur importance dans l'inclusion de notre Framework CISOaaS.

### 3.3.1. Gouvernance

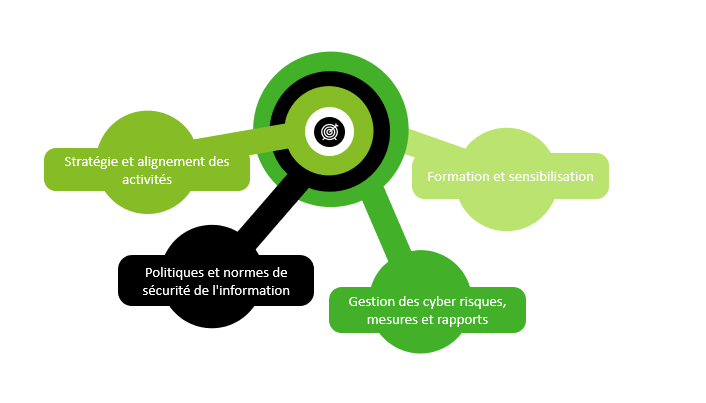
****

Figure 3.12: Catégories Gouvernance

##### - Stratégie et alignement des activités :

Cette catégorie concerne l'élaboration d'une stratégie de sécurité de l'information spécifique à l'organisation, en tenant compte de ses objectifs commerciaux. Il s'agit de s'assurer que les activités de sécurité sont alignées sur les objectifs globaux de l'entreprise.

##### - Politiques et normes de sécurité de l'information :

Ici, nous abordons l’élaboration et la maintenance des politiques de sécurité de l'information. Cela inclut la définition des normes de sécurité applicables à l'organisation pour assurer une approche cohérente et conforme.

##### - Gestion des cyber risques, mesures et rapports :

Dans cette sous-catégorie, nous nous concentrons sur l'évaluation et la gestion des risques liés à la sécurité de l'information. Cela implique l'identification des risques, l'établissement de mesures de sécurité appropriées et la création de rapports pour communiquer les résultats aux parties prenantes.

##### - Formation et sensibilisation :

Cette sous-catégorie vise à sensibiliser les employés à la sécurité de l'information à travers des programmes de formation. Il s'agit de renforcer la compréhension des bonnes pratiques de sécurité et de promouvoir une culture de sécurité au sein de l'organisation.

### 3.3.2. Risk Management

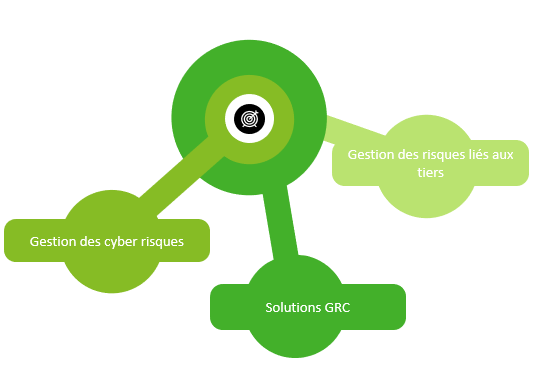
****

Figure 3.13: Catégories Risk Management

##### - Gestion des cyber risques :

Ici, l'accent est mis sur l'identification, l'évaluation et la priorisation des risques de sécurité de l'information. L'objectif est de développer des stratégies et des plans de mitigation des risques pour réduire l'exposition aux menaces.

##### - Solutions GRC (Governance, Risk, and Compliance):

Les solutions GRC sont des outils logiciels utilisés pour gérer les activités de gouvernance, de risque et de conformité. Cette sous-catégorie concerne l'adoption et l'utilisation de ces solutions pour améliorer la gestion des risques et assurer la conformité aux réglementations applicables.

##### - Gestion des risques liés aux tiers :

Cette sous-catégorie concerne l'évaluation des risques associés aux fournisseurs et aux partenaires externes de l'organisation. Il s'agit d'établir des contrats de sécurité appropriés et de mettre en place des mesures de surveillance pour atténuer les risques liés à ces relations.

### 3.3.3. Conformité

Cette catégorie se concentre sur la conformité aux normes et réglementations de sécurité spécifiques à l'industrie dans laquelle l'organisation opère. Cela implique l'évaluation de la conformité, la mise en œuvre de mesures correctives et le maintien d'un environnement conforme aux exigences légales et réglementaires.

### 3.3.4. Sécurité opérationnelle

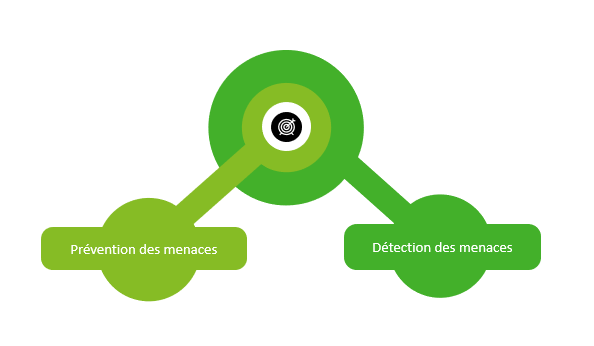
****

Figure 3.14: Catégories Sécurité Opérationnelle

#### Prévention des menaces :

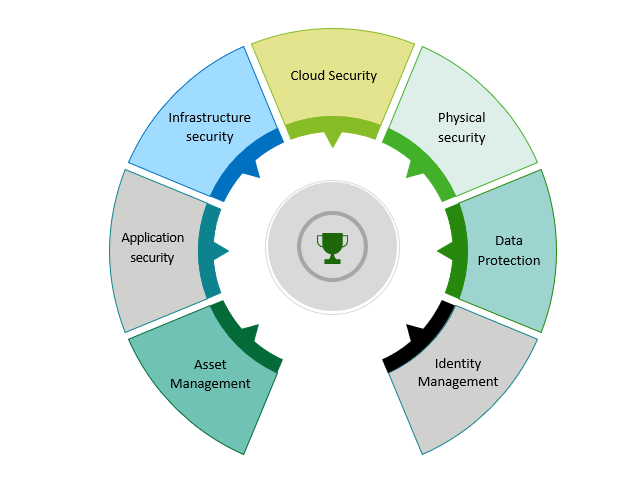


Figure 3.15: Sous catégories prévention des menaces

L'objectif de la prévention des menaces est de protéger les systèmes informatiques et les données contre les attaques malveillantes, et comprend les sous catégories suivantes.

##### Asset Management :

Cette sous-catégorie concerne la gestion des actifs de l'organisation, tels que les applications, les infrastructures et les données. Elle comprend des mesures de sécurité pour identifier, suivre et protéger ces actifs tout au long de leur cycle de vie.

##### Application security:

* Secure SDLC (Software Development Life Cycle) :

Il s'agit d'intégrer des pratiques de sécurité tout au long du cycle de vie du développement logiciel. Cela inclut l'identification des exigences de sécurité, l'utilisation de méthodologies de développement sécurisées et la réalisation de tests de sécurité pour détecter et corriger les vulnérabilités.

* Post Development Application protection :

Cette mesure de sécurité vise à protéger les applications après leur développement. Cela peut inclure des mesures telles que la surveillance de l'intégrité de l'application, la gestion des correctifs de sécurité et l'application de contrôles de sécurité supplémentaires.

##### Infrastructure security :

* System security :

Cette sous-catégorie concerne la sécurisation des systèmes informatiques de l'organisation. Cela comprend la configuration sécurisée des serveurs, des systèmes d'exploitation et des bases de données, ainsi que la mise en œuvre de mécanismes de contrôle d'accès et de protection contre les intrusions.

* Malware Protection :

Il s'agit de mettre en place des mesures de protection contre les logiciels malveillants tels que les virus, les chevaux de Troie et les ransomwares. Cela peut inclure l'utilisation d'antivirus, de pare-feu et de systèmes de détection des intrusions.

* Network Security :

Cette mesure de sécurité vise à protéger les réseaux informatiques de l'organisation contre les attaques et les intrusions. Cela peut inclure la configuration de pare-feu, la segmentation du réseau, l'utilisation de technologies de cryptage et la surveillance du trafic réseau.

* End-user Device Security :

Il s'agit de sécuriser les appareils utilisés par les utilisateurs finaux, tels que les ordinateurs de bureau, les ordinateurs portables et les appareils mobiles. Cela comprend des mesures telles que l'utilisation de mots de passe forts, la gestion des correctifs, le chiffrement des données et la sensibilisation à la sécurité des utilisateurs.

##### Cloud Security:

* Use of Managed Cloud Services:

Cette sous-sous-catégorie concerne l'utilisation de services cloud gérés pour héberger les données et les applications de l'organisation. Il s'agit de choisir des fournisseurs de services cloud fiables et d'établir des accords de sécurité appropriés.

* Cloud Strategy and Governance :

Cette mesure de sécurité concerne la planification et la gouvernance de l'utilisation du cloud au sein de l'organisation. Cela inclut la définition d'une stratégie cloud claire, la gestion des risques associés et la mise en place de contrôles appropriés.

* Data Residency and Management :

Il s'agit de s'assurer que les données de l'organisation sont stockées et gérées conformément aux réglementations en matière de confidentialité des données et de résidence des données.

* Data integrity and Availability :

Cette sous-sous-catégorie concerne la protection de l'intégrité et de la disponibilité des données stockées dans le cloud. Cela peut inclure des mesures telles que la sauvegarde des données, la réplication des données et la mise en place de mécanismes de détection d'altération des données.

* Security Solution Scalability :

Il s'agit de garantir que les solutions de sécurité utilisées dans le cloud peuvent s'adapter à l'échelle de l'organisation, en tenant compte de la croissance et des besoins changeants.

* Cloud Security Provider Support and Forensics:

Cette mesure de sécurité concerne le soutien fourni par les fournisseurs de services cloud en matière de sécurité, ainsi que la capacité de mener des enquêtes et des analyses forensiques en cas d'incident de sécurité.

* Cloud Security Provider Assurance :

Il s'agit d'évaluer et d'assurer la confiance dans les fournisseurs de services cloud en matière de sécurité. Cela peut inclure des évaluations de conformité, des audits de sécurité et des contrats de service solides.

* Cloud Security Architecture :

Cette sous-sous-catégorie se concentre sur la conception et la mise en place d'une architecture de sécurité solide pour les environnements cloud. Cela comprend la segmentation du réseau, la gestion des identités et des accès, ainsi que la gestion des clés de chiffrement.

* Allocation of security roles and responsibilities:

Il s'agit de définir clairement les rôles et les responsabilités en matière de sécurité entre l'organisation et le fournisseur de services cloud, afin de garantir une gestion efficace de la sécurité des données et des applications.

* Cloud Security Assessment :

Cette mesure de sécurité vise à évaluer régulièrement la sécurité des environnements cloud de l'organisation, en utilisant des méthodes telles que les tests de pénétration, les évaluations de conformité et les analyses des vulnérabilités.

##### Physical security :

Cette sous-catégorie concerne la sécurité physique des installations et des équipements de l'organisation. Elle inclut des mesures de contrôle d'accès, de surveillance, de gestion des événements physiques et de protection des médias amovibles.

##### Data Protection :

Cette sous-catégorie se concentre sur la protection des données sensibles de l'organisation. Elle comprend des mesures telles que la prévention des pertes de données, la gestion du cycle de vie de l'information, la confidentialité des données, la classification de l'information et l'utilisation de techniques de chiffrement pour protéger les données.

##### Identity Management :

Cette sous-catégorie concerne la gestion des identités et des accès des utilisateurs au sein de l'organisation. Elle comprend des mesures telles que la gestion du cycle de vie des identités, le contrôle d'accès utilisateur basé sur les rôles et les privilèges, ainsi que le contrôle d'accès des utilisateurs privilégiés.

#### Détection des menaces :



Figure 3.16: Sous-catégories détection des menaces

L'objectif de la détection des menaces est d'identifier rapidement les activités suspectes et les signes de compromission afin de prendre des mesures appropriées pour contrer les menaces potentielles.

##### Penetration Testing & Vulnerability Scanning:

* Security Testing Schedule:

Il s'agit d'établir un calendrier régulier pour effectuer des tests de sécurité, tels que les tests de pénétration et les analyses de vulnérabilités. Cela permet d'identifier les failles de sécurité potentielles dans les systèmes et les applications de l'organisation.

* Testing Policy (Internal, external, host, cloud data leakage and hunting):

Cette mesure de sécurité consiste à définir une politique de tests de sécurité claire, en spécifiant les types de tests à effectuer (internes, externes, ciblant l'hébergement, la fuite de données dans le cloud, etc.) et les objectifs à atteindre.

* Testing Tools :

Il s'agit de sélectionner et d'utiliser des outils spécialisés pour effectuer les tests de pénétration et les analyses de vulnérabilités de manière efficace. Ces outils aident à identifier les faiblesses de sécurité et à proposer des solutions pour les corriger.

##### Cyber Threat Intelligence:

* Collection of CTI:

Cette sous-sous-catégorie concerne la collecte d'informations sur les menaces cybernétiques provenant de différentes sources, telles que les rapports d'incidents, les bases de données de vulnérabilités et les sources d'intelligence externes.

* Analysis and Sharing of CTI:

Il s'agit d'analyser les informations sur les menaces cybernétiques collectées afin de comprendre les tactiques, les techniques et les procédures utilisées par les attaquants. Ces informations sont ensuite partagées avec les équipes de sécurité pour renforcer la posture de sécurité de l'organisation.

* Use of CTI :

Cette mesure de sécurité consiste à utiliser les informations sur les menaces cybernétiques pour prendre des décisions éclairées en matière de sécurité, telles que l'ajustement des politiques de sécurité, la mise à jour des outils de sécurité et la sensibilisation des utilisateurs.

* Threat Profile Monitoring :

Il s'agit de surveiller en continu les profils de menaces émergentes afin de détecter rapidement de nouvelles tendances et de prendre des mesures préventives appropriées.

##### Brand Protection :

* Brand Monitoring :

Cette mesure de sécurité consiste à surveiller et à protéger la réputation de la marque de l'organisation en ligne. Cela peut inclure la surveillance des mentions de la marque sur les médias sociaux, les sites Web et les forums, afin de détecter et de prévenir les activités frauduleuses ou nuisibles.

* Social Media Monitoring :

Il s'agit de surveiller les activités liées à la marque sur les plateformes de médias sociaux, afin d'identifier les menaces potentielles, les faux profils, les tentatives de phishing et les atteintes à la réputation de la marque.

* Communications :

Cette mesure de sécurité concerne la protection des communications de l'organisation contre les attaques, telles que le vol d'informations sensibles ou la falsification de messages. Cela peut inclure l'utilisation de chiffrement, d'authentification forte et de politiques de sécurité des communications.

##### Social Event Monitoring:

* SIEM Solution, Architecture and Deployment:

Cette mesure de sécurité concerne l'utilisation d'une solution SIEM (Security Information and Event Management) pour la collecte, la corrélation et l'analyse des événements de sécurité. Cela inclut la conception de l'architecture SIEM, son déploiement et son intégration avec d'autres outils de sécurité

* Use Case Library and Lifecycle Maintenance:

Il s'agit de créer une bibliothèque de cas d'utilisation SIEM qui définissent les événements de sécurité à surveiller et les actions à prendre en cas de détection d'activités suspectes. Cette bibliothèque est régulièrement mise à jour pour s'adapter aux nouvelles menaces et aux changements dans l'environnement de sécurité.

* Log Collection, Correlation and Protection :

Cette sous-sous-catégorie concerne la collecte, la corrélation et la protection des journaux (logs) générés par les différents systèmes et applications de l'organisation. Cela permet d'identifier les activités malveillantes, de détecter les anomalies et de répondre aux incidents de sécurité.

* Operating/Support Model, SOC Coverage, Talent, and Staffing:

Il s'agit de mettre en place un modèle opérationnel et de support efficace pour le fonctionnement du Centre des Opérations de Sécurité (SOC). Cela comprend la planification des horaires de couverture du SOC, le recrutement et la formation du personnel qualifié en matière de sécurité.

* Threat Intelligence Integration and Insider Threat Monitoring:

Cette mesure de sécurité consiste à intégrer les informations sur les menaces provenant de sources d'intelligence externe dans le processus de surveillance des événements de sécurité. Elle comprend également la surveillance des menaces internes et des comportements suspects des utilisateurs internes.

* End Point Breach Detection :

Il s'agit de mettre en place des mécanismes de détection des atteintes aux points de terminaison (Endpoint), tels que les ordinateurs de bureau, les ordinateurs portables et les appareils mobiles. Cela permet de détecter les activités malveillantes sur ces dispositifs et de prendre des mesures pour y remédier.

* File Integrity Monitoring :

Cette mesure de sécurité consiste à surveiller en continu l'intégrité des fichiers critiques de l'organisation. Cela permet de détecter toute modification non autorisée des fichiers et d'alerter sur d'éventuelles atteintes à la sécurité.

##### Patch & Vulnerability Management:

* Vulnerability Review and Analysis:

Il s'agit de passer en revue et d'analyser les vulnérabilités identifiées dans les systèmes et les applications de l'organisation. Cela permet de comprendre les risques associés à ces vulnérabilités et de prioriser les actions correctives.

* Vulnerability/Patch Deployment Planning :

Cette mesure de sécurité concerne la planification et la gestion du déploiement des correctifs de sécurité pour remédier aux vulnérabilités identifiées. Cela inclut l'établissement d'un processus de déploiement, la coordination avec les équipes responsables et le suivi des progrès.

* Vulnerability and Patch Mitigation Tracking:

Il s'agit de suivre et de vérifier l'efficacité des mesures prises pour atténuer les vulnérabilités et appliquer les correctifs de sécurité. Cela permet de s'assurer que les vulnérabilités sont traitées de manière appropriée et que les correctifs sont appliqués dans les délais requis.

* Vulnerability Re-Testing :

Cette mesure de sécurité consiste à retester les vulnérabilités après l'application des correctifs pour vérifier si elles ont été efficacement corrigées. Cela permet de s'assurer que les correctifs ont été déployés avec succès et que les vulnérabilités ne sont plus présentes.

##### Gestion des incidents :

* Simulations de cyber incidents et de crise :

Cela consiste à mener des exercices et des scénarios simulés pour simuler des incidents cybernétiques et des situations de crise. Ces simulations aident à tester l'efficacité des plans de réponse aux incidents, à identifier les lacunes et à former l'équipe d'intervention aux incidents sur la manière de gérer des incidents réels.

* Cadre, processus et livrets de gestion des incidents :

Cela comprend l'établissement d'un cadre pour la gestion des incidents, la définition des processus de gestion des incidents et la création de livrets de réponse aux incidents. Le cadre fournit une approche structurée pour gérer et répondre aux incidents de sécurité, tandis que les livrets décrivent les instructions et les lignes directrices étape par étape pour des types spécifiques d'incidents.

* Indicateurs de performance et structures de reporting des incidents :

Cela implique la définition des indicateurs de performance et des indicateurs clés (KPI) pour mesurer l'efficacité et l'efficience des processus de gestion des incidents. Cela comprend également l'établissement de structures de reporting pour suivre et communiquer les indicateurs d'incidents aux parties prenantes pertinentes, telles que la direction et les organismes de réglementation.

* Rôles et responsabilités :

Cela consiste à définir et attribuer les rôles et responsabilités au sein de l'équipe d'intervention aux incidents. Cela inclut l'identification des membres de l'équipe d'intervention aux incidents, de leurs rôles et des tâches et responsabilités spécifiques dont ils sont responsables pendant la réponse aux incidents.

* Communication externe :

Cela se concentre sur l'établissement de protocoles et de canaux de communication pour la communication externe lors d'incidents de sécurité. Cela comprend la définition de la manière et du moment de communiquer avec des parties externes, telles que les clients, les partenaires, les organismes chargés de l'application des lois et les organismes de réglementation, pour fournir des mises à jour rapides et précises sur l'incident.

* Formation et sensibilisation :

Cela comprend la réalisation de programmes de formation et de campagnes de sensibilisation pour sensibiliser les employés et les parties prenantes aux processus de gestion des incidents, à leurs rôles et responsabilités, ainsi qu'à l'importance d'un signalement et d'une réponse rapides aux incidents de sécurité. L'objectif est de créer une culture de sensibilisation à la sécurité et de préparation au sein de l'organisation.

La détection des menaces comprend donc un ensemble de mesures visant à identifier les vulnérabilités, à surveiller les événements de sécurité, à détecter les menaces émergentes, à protéger la marque de l'organisation et à gérer les correctifs de sécurité. Ces mesures contribuent à renforcer la posture de sécurité de l'organisation et à minimiser les risques liés aux attaques et aux incidents de sécurité.

### 3.3.5. Résilience

#### - *Continuité d'activité :*

Cette catégorie concerne la préparation à la continuité des activités en cas de perturbation majeure. Cela comprend l'identification des processus critiques, la mise en place de plans de continuité et la réalisation de tests pour assurer la capacité de l'organisation à continuer ses opérations.

#### - Reprise après sinistre :

Ici, nous abordons les mesures prises pour la reprise des opérations après un sinistre majeur. Cela implique la mise en place de plans de reprise, la sauvegarde et la restauration des données, ainsi que la planification des infrastructures de secours.

#### - *Gestion des incidents :*

Cette sous-catégorie se concentre sur la gestion des incidents de sécurité. Cela inclut la détection, l'évaluation, la réponse et la récupération des incidents de sécurité, ainsi que la communication avec les parties prenantes et la mise en place de mesures d'amélioration continue.

### 3.3.6. Project Delivery Lifecycle :

Cette catégorie concerne l'intégration des principes de sécurité de l'information tout au long du cycle de vie de la livraison des projets. Cela inclut la définition des exigences de sécurité, l'évaluation des risques, la gestion des contrôles de sécurité et l'assurance qualité pour garantir que les projets sont livrés en tenant compte de la sécurité dès le départ.

Ces services, catégories et sous-catégories couvrent un large éventail de domaines de sécurité de l'information. Ils sont conçus pour aider les organisations à gérer les risques, à assurer la conformité, à prévenir les menaces, à renforcer la résilience et à intégrer la sécurité dans leurs projets.

## **Conclusion**

En conclusion, nous avons vu les six services clés que nous devons fournir pour offrir une solution complète de CISO en tant que service. Ces services comprennent la sécurité opérationnelle, la détection des menaces, la gestion des incidents, la gouvernance et la conformité, la gestion des risques et la formation et la sensibilisation.

Ces services sont conçus pour répondre aux défis complexes de la sécurité de l'entreprise et offrir une protection efficace contre les menaces actuelles et futures. Dans le prochain chapitre, nous détaillerons les fonctionnalités et les avantages de notre solution, notamment à travers notre Dashboard qui permet une surveillance en temps réel et une gestion optimisée des risques de sécurité.

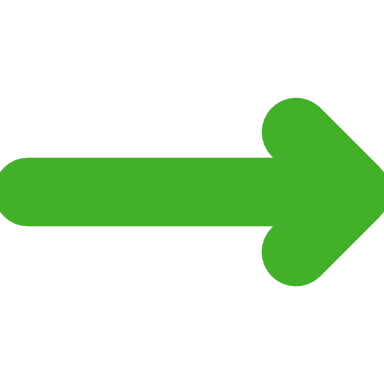
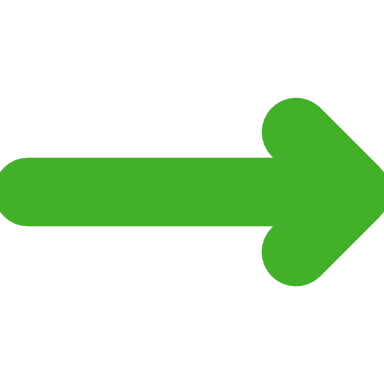
# **Chapitre 4 : Réalisation du Projet**

## **Introduction**

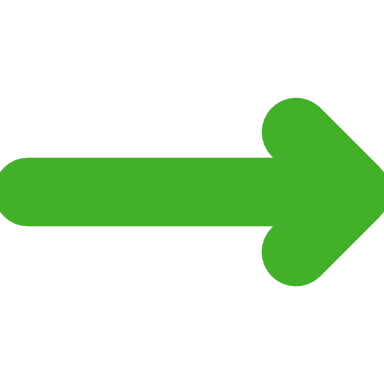
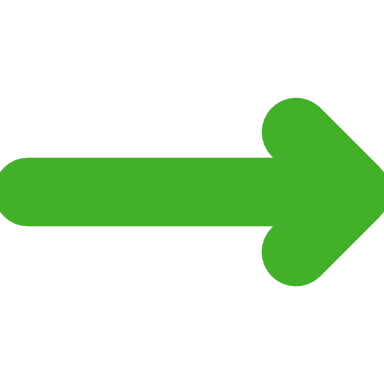
Dans ce chapitre, nous aborderons la mission client à laquelle j'ai été intégrée pendant ma période de stage. Bien que nous ne puissions pas divulguer les détails spécifiques de notre participation en raison des exigences de confidentialité de notre organisme d'accueil et de la sensibilité du client concernant cette mission, cela ne nous empêchera pas de présenter notre rôle et les tâches que nous avons réalisées dans le cadre de cette mission.

## **Contexte et objectif de la mission**

Au cours de mon stage de six mois, j'ai eu l'opportunité exceptionnelle de participer activement à une mission passionnante en tant que membre de l'équipe CISOaaS, au service d'un client français de renom. L'objectif principal de cette mission stratégique était de fournir à notre client une expertise hautement qualifiée en matière de cybersécurité afin de faire face aux menaces de plus en plus sophistiquées qui pèsent sur leur environnement numérique, ainsi que de réduire les coûts associés à la mise en place et à la gestion d'une équipe de sécurité interne.

Notre mission a été menée en respectant le planning établi, qui nous a guidés tout au long de notre parcours. Nous avons suivi méticuleusement les différentes étapes et les délais prévus, ce qui nous a permis d'atteindre nos objectifs de manière efficace et efficiente. Grâce à cette planification rigoureuse, nous avons pu gérer nos ressources et nos activités de manière optimale, assurant ainsi le bon déroulement de notre mission.

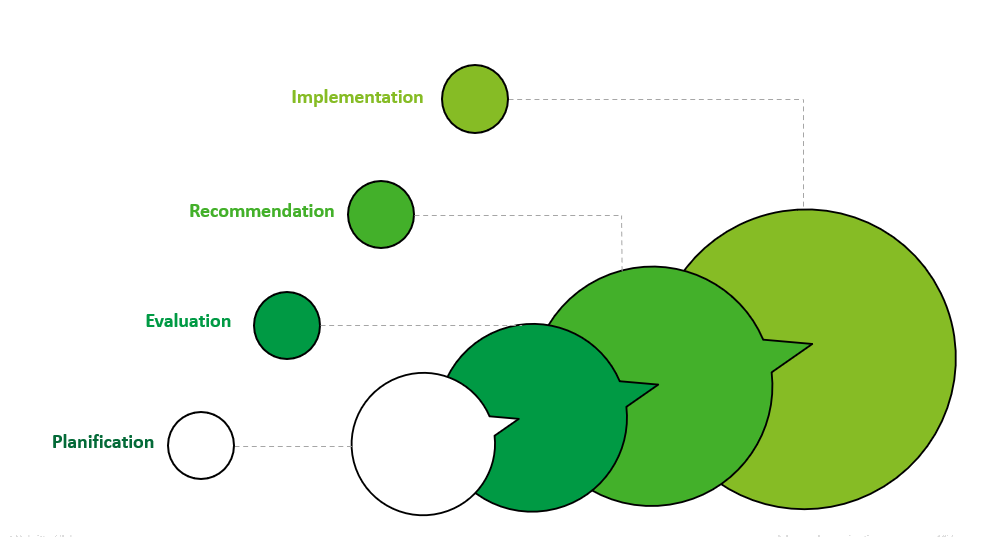
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Mai | | | | | Juin | | | | Juillet | | | | |
| **Phases** | 1 | 8 | 15 | 22 | 29 | 5 | 12 | 19 | 26 | 3 | 10 | 17 | 24 | 31 |
| Réunion de Kick-off |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Planification des entretiens |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Déroulement des entretiens |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Revue des réponses |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Formulation des constats |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Identification des écarts |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Présentation des résultats et du Dashboard |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Elaboration des recommandations |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Implémentation des recommandations proposées |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Réévaluation des contrôles implémentés |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Présentation du résultat final |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Clôture du projet |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Tableau 2: Planning mission

En travaillant en étroite collaboration avec notre client, nous avons développé une approche personnalisée pour répondre à ses besoins spécifiques en matière de sécurité. Notre priorité était d'assurer une protection optimale des actifs informationnels de l'entreprise, tout en minimisant les risques et en garantissant une stricte conformité avec les normes et réglementations en vigueur.

## **Méthodologie suivie pendant la mission**

La mission en question se divise en 4 parties que je détaillerai par la suite. Ces parties sont basées principalement sur l’approche que nous avons proposée et que j’ai abordé dans le chapitre précédent.

Figure 4.1: Méthodologie suivie pendant la mission

### **Planification**

Notre mission a commencé par une réunion de Kick-off qui a eu lieu le 8 mai, au cours de laquelle nous avons travaillé en étroite collaboration avec le client pour valider les objectifs et le périmètre du projet. Cette réunion nous a également permis de définir le budget alloué, les ressources nécessaires et d'identifier les parties prenantes impliquées, ainsi que de clarifier les rôles et responsabilités de chacun. Nous avons pu élaborer un planning détaillé, qui a servi de feuille de route pour l'ensemble du projet, ainsi qu’un document de cadrage qui englobe le contexte, le budget et les ressources nécessaires.

Cette phase initiale a été très importante pour établir une base solide et une compréhension mutuelle entre notre équipe et le client. Nous avons pris le temps d'écouter attentivement les besoins et les attentes du client, en tenant compte des contraintes et des spécificités de son environnement.

### **Evaluation**

Une fois notre planning établi, nous avons entamé la deuxième phase cruciale de notre mission : évaluer attentivement l'efficacité des mesures de sécurité mises en place par notre client pour protéger ses informations sensibles et ses systèmes d'information. Pour ce faire, nous avons programmé des entretiens avec les responsables des départements clés liés à la sécurité chez notre client qui ont été identifiés lors de l’étape de la définition du périmètre.

Lors de ces entretiens, nous avons utilisé notre Framework qui comprend une liste de questions couvrant les 6 services préalablement discutés. Cette approche méthodique nous a permis d'explorer en détail les aspects pertinents de la sécurité et de recueillir les informations nécessaires.

Grâce à cette méthodologie rigoureuse, nous avons fourni à notre client une évaluation complète de sa sécurité, lui permettant de prendre des décisions éclairées pour renforcer sa posture globale en matière de sécurité. À la fin de cette étape, nous avons accompli une tâche importante en obtenant une liste exhaustive pour chaque service, comprenant une réponse précise à chaque question ainsi qu'une attribution de score.

Nous avons consciencieusement recueilli et enregistré les réponses obtenues lors des entretiens avec les responsables des départements clés de sécurité chez notre client. En nous appuyant sur notre Framework, nous avons veillé à aborder en profondeur chaque question et à documenter les informations pertinentes.

Cette approche méthodique nous a permis d'évaluer objectivement l'efficacité des mesures de sécurité en place chez notre client. En attribuant des scores appropriés à chaque réponse, nous avons pu quantifier et comparer les performances de chaque service évalué.

La liste complétée, avec les réponses précises et les scores alloués, représente un outil précieux pour nous. Elle offre une vue d'ensemble claire de la situation actuelle de la sécurité et permet d'identifier les domaines nécessitant une attention particulière ou des améliorations. Ci-dessous le rendu final du service de la Gouvernance à la suite des entretiens effectués entre le 15 et 23 mai.

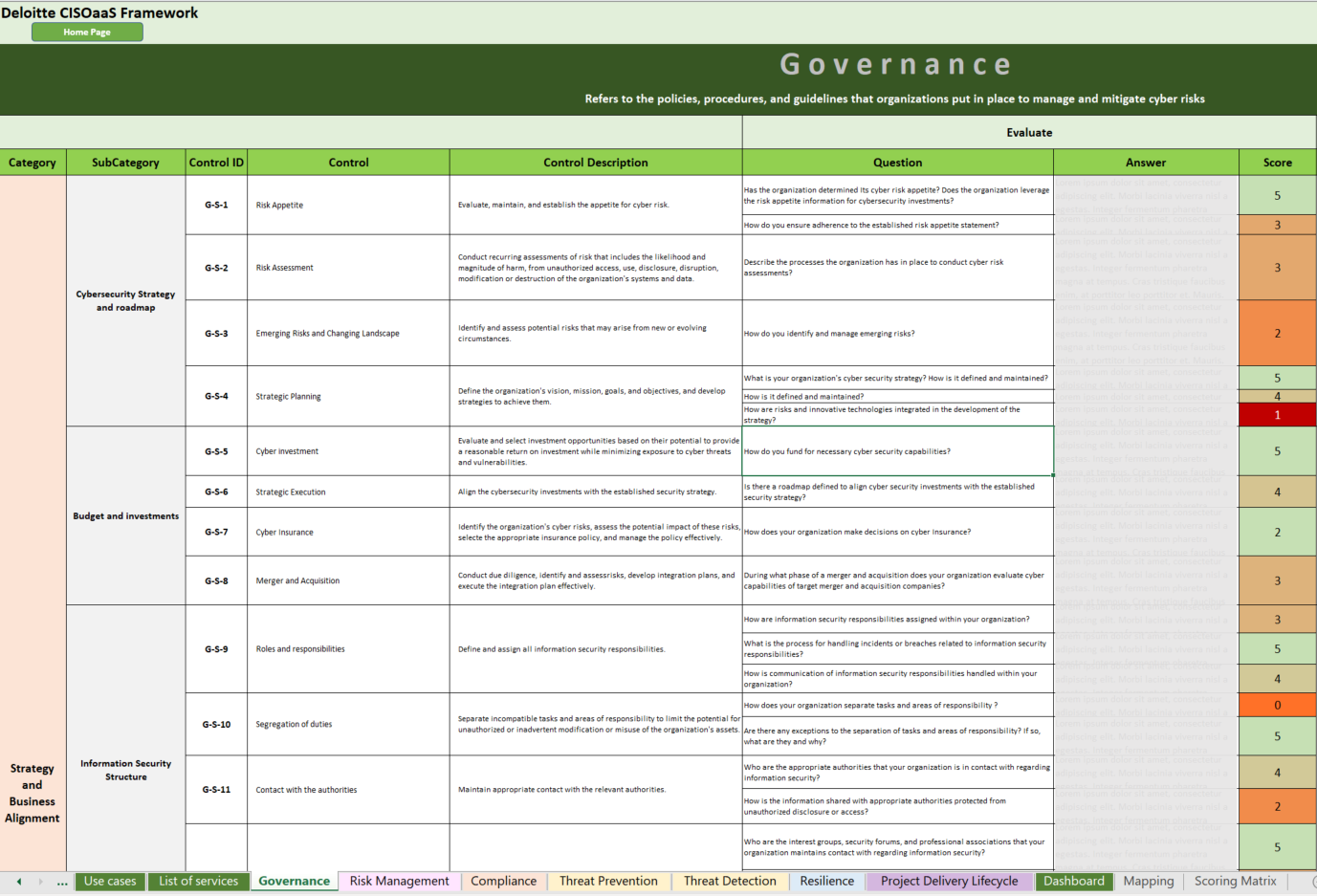


Figure 4.2: Evaluation service Gouvernance

Après avoir mené neuf entretiens avec le département de sécurité de notre client, nous avons organisé une réunion en interne avec notre équipe afin de dresser le constat d'audit et d'établir une évaluation. Dans le cadre de la confidentialité des informations, nous ne pourrons aborder ici qu'un exemple de constat lié au service de la gouvernance.

Après avoir réalisé une analyse approfondie des politiques de sécurité de l'information mises en place au sein de l'organisation cliente, plusieurs constats majeurs ont été identifiés.

Tout d'abord, les politiques de sécurité de l'information sont globalement bien définies et documentées, reflétant un engagement solide de l'organisation envers la protection des données et des actifs informatiques. Elles comprennent des procédures claires concernant l'accès aux informations sensibles, la classification des données et la gestion des risques liés à la cybersécurité.

Cependant, malgré cette documentation adéquate, il a été constaté un manque de communication efficace au sein de l'organisation. Les employés ne semblent pas tous avoir été informés de l'existence de ces politiques et de leurs responsabilités en matière de sécurité de l'information. Il est recommandé à l'organisation d'établir un plan de communication formel pour sensibiliser tous les employés aux politiques de sécurité, afin de s'assurer de leur compréhension et de leur respect.

De plus, bien que des mesures de contrôle d'accès aient été mises en place, il a été observé des faiblesses dans la mise en œuvre de ces contrôles. Certains employés disposent d'autorisations excessives, ce qui augmente les risques de fuites de données ou d'accès non autorisés. Il est donc fortement recommandé à l'organisation de revoir et de renforcer les mécanismes de contrôle d'accès afin de limiter les privilèges et de garantir un accès approprié aux données sensibles.

Il est important de souligner que cet exemple de constat ne couvre qu'un aspect spécifique d’un contrôle de la gouvernance. D'autres constats ont été formulés pour d'autres contrôles du Framework CISO as a Service, qui ne peuvent être abordés ici en raison des exigences en matière de confidentialité. Ces constats serviront de base pour soutenir notre client dans son parcours d'amélioration continue de sa posture de cybersécurité.

Après avoir finalisé les constats, nous avons organisé une réunion avec notre client pour lui présenter notre évaluation et nos observations. Nous avons ensuite entrepris une analyse approfondie des différences entre l'état actuel de la sécurité de notre client et les contrôles recommandés définis dans notre modèle de maturité cible.

Pour mener cette analyse, nous avons comparé les mesures de sécurité existantes chez notre client avec les meilleures pratiques et les normes de sécurité reconnues à l'échelle de l'industrie. Nous avons identifié les différences et les manques entre l'état actuel de sécurité et l'état de maturité cible que nous visons pour notre client.

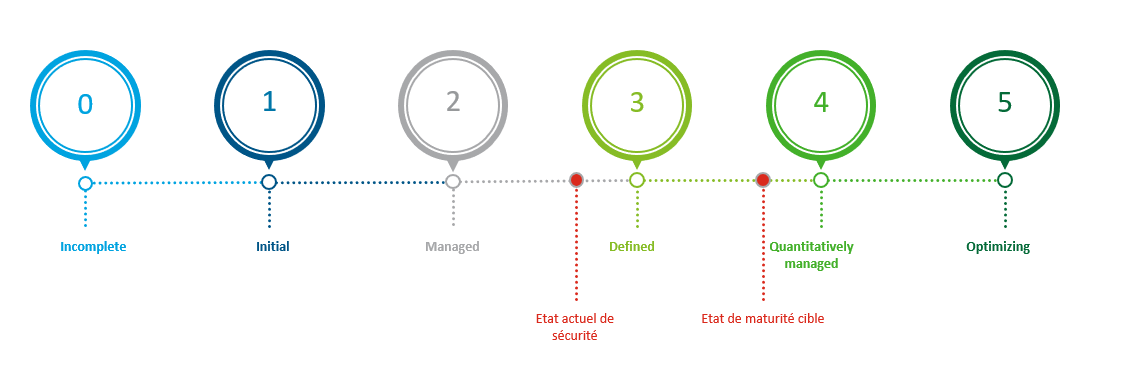


Figure 4.3: Représentation du niveau de maturité

Dans le but de visualiser les résultats et faciliter le processus d'évaluation lors de cet évaluation, nous avons mis en place un tableau de bord automatisé. Ce tableau de bord joue un rôle essentiel dans le calcul du niveau de maturité de chaque catégorie et service, permettant ainsi d'afficher le niveau de maturité global de notre client.

Le tableau de bord utilise des données collectées lors de l'entretien avec les parties prenantes, ainsi que les réponses aux questions définies dans notre Framework. Il applique des algorithmes et des formules spécifiques pour évaluer et attribuer des scores à chaque catégorie et service.

Notre Dashboard repose sur plusieurs indicateurs clés de performance (KPI). Tout d'abord, nous présentons le niveau de maturité global, suivi d'une comparaison entre les différents services évalués. Cette première partie offre un résumé de l'état actuel de maturité par rapport à l'état idéal. Il est important de noter que le passage de l'état actuel à l'état cible est défini en fonction des objectifs, du budget et des spécificités de chaque client. Nous veillons à ce que la transition soit réaliste et réalisable.

Dans la deuxième partie du Dashboard, nous proposons une visualisation détaillée de chaque service individuellement. Nous mettons en avant quatre KPI :

* Le nombre de questions auxquelles des réponses ont été apportées lors de l'évaluation, ainsi que celles qui sont restées sans réponse.
* Le niveau de maturité actuel du service, qui nous donne une indication claire de son degré d'avancement par rapport à l'état cible.
* Le niveau de maturité de chaque catégorie spécifique du service, ce qui nous permet de cibler les domaines à améliorer pour chaque service.
* Le statut de la mise en œuvre des recommandations que nous allons entamer immédiatement.

Ces informations présentées de manière claire et visuelle sur notre Dashboard fournissent à notre client une vision complète de l'état de chaque service évalué, facilitant ainsi l'identification des axes d'amélioration prioritaires.

Cette approche automatisée a considérablement facilité l'analyse des résultats et a permis une évaluation plus précise de la posture de sécurité de notre client. Le tableau de bord fournit une vue d'ensemble facilement compréhensible, ce qui facilite les discussions et les prises de décision concernant les actions à entreprendre pour renforcer la sécurité.

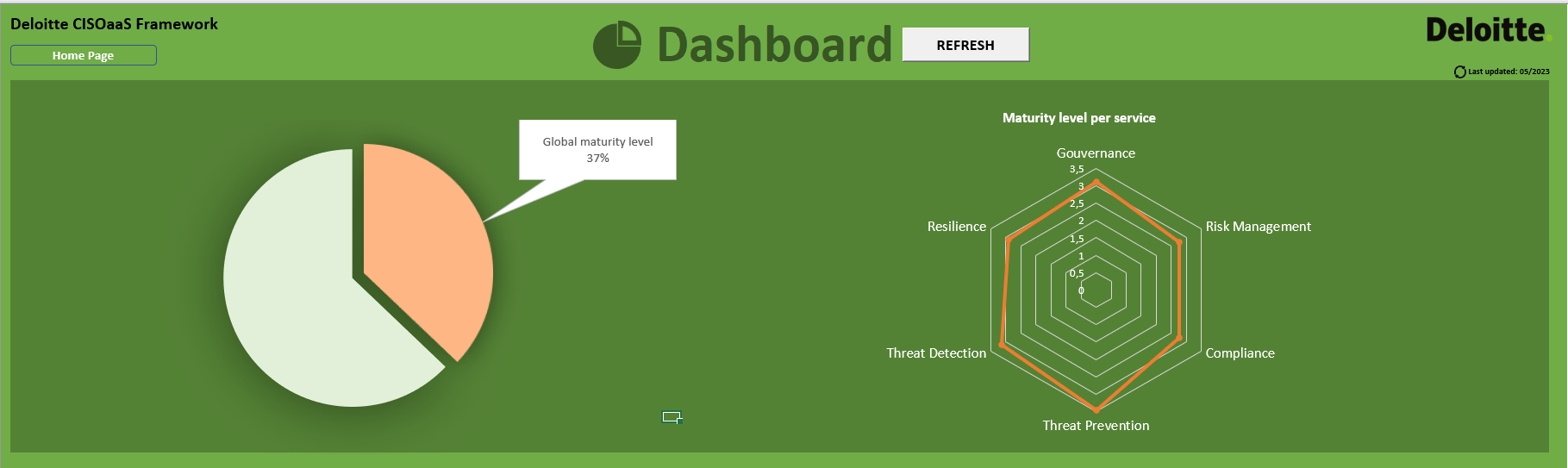


Figure 4.4: Aperçu du niveau de maturité global sur le Dashboard



Figure 4.5: Aperçu détaillé des services sur le Dashboard



Figure 4.6: Aperçu détaillé des services sur le Dashboard

En résumé, grâce à notre tableau de bord automatisé, nous avons pu évaluer le niveau de maturité de la sécurité de notre client de manière efficace et objective. Cette visualisation claire des résultats a été un atout majeur pour notre équipe et pour le client, permettant une meilleure compréhension de la situation actuelle et la mise en place de mesures d'amélioration ciblées.

### **4.2.3. Recommandation et implémentation**

Une fois l'évaluation de la posture de sécurité terminée et le niveau de maturité déterminé, nous avons organisé une réunion pour présenter les résultats à notre client. Cette réunion a été l'occasion de partager en détail les conclusions de notre évaluation et de discuter des prochaines étapes, à savoir la phase de recommandation et d'implémentation.

Lors de cette réunion, nous avons présenté les résultats de manière claire et concise, mettant en évidence les forces et les faiblesses identifiées dans la posture de sécurité de notre client. Nous avons discuté des implications de ces résultats et de l'importance de mettre en place des mesures appropriées pour renforcer la sécurité.

Nous avons également abordé la phase de recommandation, au cours de laquelle nous élaborerons des recommandations détaillées et personnalisées pour améliorer la posture de sécurité de notre client. Ces recommandations seront basées sur les approches optimales proposées sur notre Framework, ainsi que les meilleures pratiques de l'industrie tout en étant adaptées aux besoins spécifiques de notre client.

Après avoir partagé les recommandations avec notre client, nous entamerons la phase d'implémentation. Cette phase impliquera la mise en œuvre des mesures de sécurité recommandées, en collaboration étroite avec notre client. Nous travaillerons ensemble pour élaborer un plan d'action, définir les responsabilités et les échéances, et suivre de près le processus de mise en place des mesures de sécurité.

Les phases de recommandation et d'implémentation se dérouleront sur les mois prochains, pendant lesquels nous travaillerons activement pour renforcer la sécurité de notre client. Nous resterons en contact régulier avec notre client, fournissant des mises à jour, répondant à ses questions et ajustant notre approche en fonction de ses besoins et de son environnement spécifique.

En somme, la réunion de restitution des résultats marque le début de la phase de recommandation et d'implémentation, où nous travaillerons en étroite collaboration avec notre client pour améliorer sa posture de sécurité. Nous sommes engagés à fournir des recommandations de qualité et à mettre en place des mesures efficaces pour assurer la sécurité de notre client dans les mois à venir.

## **Conclusion**

En conclusion, ce chapitre a couvert ma participation active à la mission client en tant que CISOaaS. Nous avons abordé la mise en place du contexte et des objectifs de la mission, ainsi que la méthodologie que nous avons adoptée pour atteindre ces objectifs. Cependant, en raison de la confidentialité des informations et du fait que la mission est toujours en cours, nous n'avons pas pu fournir de détails approfondis.

# **Conclusion générale**

En conclusion, ce rapport de stage a détaillé le projet réalisé dans le cadre du PFE au Deloitte Morocco Cyber Center. L'objectif du projet était de développer un toolkit basé sur une approche et un Framework pour offrir des services de CISO en tant que service. Les quatre chapitres présentent l'entreprise d'accueil, décrivent le contexte général du projet, examinent en détail les différentes étapes du projet et mettent en évidence les réalisations concrètes.

Ce projet a été une occasion enrichissante de mettre en pratique les connaissances théoriques acquises tout au long de notre formation. Il nous a permis de travailler en étroite collaboration avec des professionnels chevronnés de la cybersécurité et de comprendre les défis réels auxquels les organisations sont confrontées pour protéger leurs informations sensibles.

Une perspective importante pour l'amélioration continue de ce toolkit est d'impliquer les utilisateurs finaux et les parties prenantes dans le processus de développement et de les inclure dans le cycle de retour d'information. Leurs commentaires et leurs besoins spécifiques permettront d'enrichir et d'affiner le toolkit afin qu'il réponde de manière optimale aux exigences du marché.

Il est également essentiel de se tenir au courant des évolutions technologiques et des nouvelles tendances en matière de cybersécurité. Une vigilance et un suivi constants des nouvelles méthodes d'attaque et des meilleures pratiques permettront à notre toolkit de rester pertinent et efficace face à des menaces en constante évolution.

Enfin, l'apprentissage continu et l'échange d'expériences au sein de la communauté de la cybersécurité contribueront également à l'amélioration constante du toolkit. La participation à des conférences, des forums et des groupes de travail nous permettra de nous tenir au courant des dernières évolutions et de bénéficier des connaissances et de l'expertise des professionnels du secteur.

Pour finir, ce projet de développement du toolkit CISO as a Service a été une expérience stimulante et formatrice. Il nous a permis d'appréhender les véritables enjeux de la cybersécurité dans le monde de l'entreprise et de contribuer à la protection des informations sensibles. La perspective d'une amélioration continue du toolkit offre des opportunités passionnantes pour répondre à l'évolution des besoins des organisations et continuer à assurer une protection solide contre les cybermenaces.

# **Bibliographie**

**Sources internes Deloitte**

[What Is a CISO? Chief Information Security Officer - Cisco](https://www.cisco.com/c/en/us/products/security/what-is-ciso.html)

[What is a CISO (chief information security officer)? Definition from SearchSecurity (techtarget.com)](https://www.techtarget.com/searchsecurity/definition/CISO-chief-information-security-officer)

[What is a CISO? Responsibilities and requirements for this vital role | CSO Online](https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html)

[The CISO challenge of budgeting – Intelligent CISO](https://www.intelligentciso.com/2021/09/09/the-ciso-challenge-of-budgeting/)

[Cybersecurity Framework | NIST](https://www.nist.gov/cyberframework)

[An Introduction to COBIT | Joe The IT Guy](https://www.joetheitguy.com/an-introduction-to-cobit/)

[ISO 27001, the Information Security Standard | IT Governance USA](https://www.itgovernanceusa.com/iso27001)

[ISO 27001 | Spécialistes ISO | IMSM FR](https://www.imsm.com/fr/iso-27001/?keyword=iso%2027001&matchtype=e&network=o&device=c&utm_term=iso%2027001&utm_campaign=LOL+-+Search+-+FR+27001&utm_source=bing&utm_medium=cpc&hsa_acc=4448709510&hsa_cam=11767528072&hsa_grp=1317216590140884&hsa_ad=&hsa_src=o&hsa_tgt=kwd-82326971360127:loc-66&hsa_kw=iso%2027001&hsa_mt=e&hsa_net=adwords&hsa_ver=3&msclkid=4305b46ee8ce1145f839d018e6172923)

[What is risk management? | IBM](https://www.ibm.com/topics/risk-management)

[What Is Cybersecurity Compliance | CompTIA](https://www.comptia.org/content/articles/what-is-cybersecurity-compliance)

[ISO 27001 Annex : 12 Operations Security | Infosavvy Security and IT Management Training (info-savvy.com)](https://info-savvy.com/iso-27001-annex-12-operations-security/)

[ISO 27001 Annex A.12: Operations Security | Hicomply](https://hicomply.com/resource-hub/iso-27001-annex-a-12-operations-security)

[Threat Prevention - How to Stop Cyber Threats? - Cisco](https://www.cisco.com/c/en/us/products/security/what-is-threat-prevention.html)

[Advanced Threat Prevention - Palo Alto Networks](https://www.paloaltonetworks.com/network-security/advanced-threat-prevention)

[Threat Prevention (paloaltonetworks.com)](https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention)

[Threat Detection and Threat Prevention: Tools and Tech (cynet.com)](https://www.cynet.com/advanced-threat-protection/threat-detection-and-threat-prevention-tools-and-tech/)

[What Is Security Resilience? - Cisco](https://www.cisco.com/c/en/us/products/security/what-is-security-resilience.html)

[What is cyber resilience? | Definition from TechTarget](https://www.techtarget.com/whatis/definition/cyber-resilience)

[What Is The Project Life Cycle: 5 Phases & Why It’s Still Important (thedigitalprojectmanager.com)](https://thedigitalprojectmanager.com/projects/pm-methodology/project-management-life-cycle/)

<https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r5-control-catalog.xlsx>

[What is a CISO as a service (CISOaaS)? Definition from SearchSecurity (techtarget.com)](https://www.techtarget.com/searchsecurity/definition/CISO-as-a-service-vCISO-virtual-CISO-fractional-CISO)

<https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx>

[What is CISO as a Service? - Synoptek](https://synoptek.com/about-us/faq/what-is-ciso-as-a-service/)

[CISO-as-a-Service | Enterprise Recovery (deloitte.com)](https://www2.deloitte.com/dk/da/pages/risk/cyber-risk/enterprise-recovery/ciso-as-a-service.html)

[FW-MG-NISTCSF& ISO-IEC27001\_0.pdf (imprivata.com)](https://www.imprivata.com/sites/imprivata/files/2021-03/FW-MG-NISTCSF%26%20ISO-IEC27001_0.pdf)

# **Annexes**

Programmes VBA du toolkit

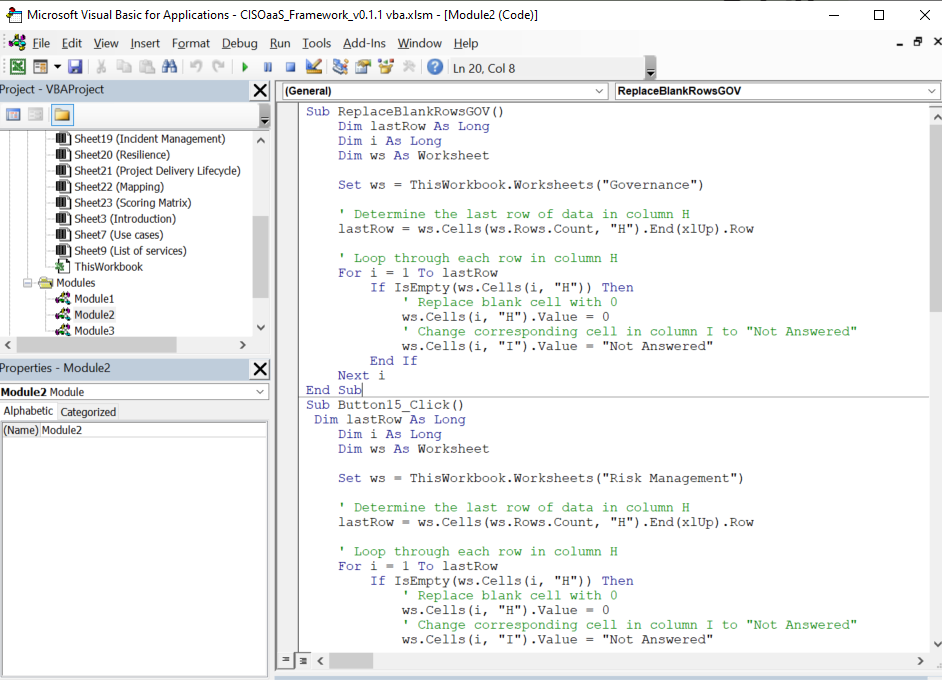


Figure A.1: Programme VBA service G et RM

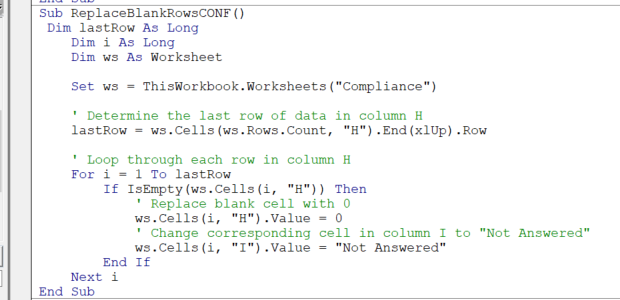


Figure A.2: Programme VBA service Compliance

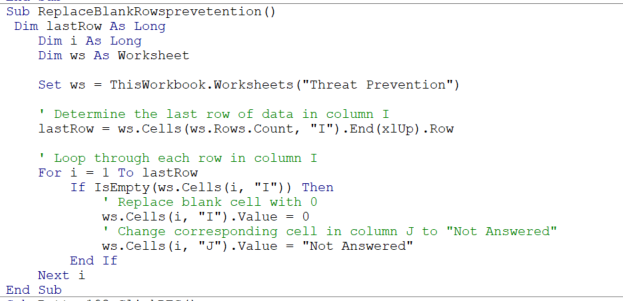


Figure A.3: Programme VBA TP

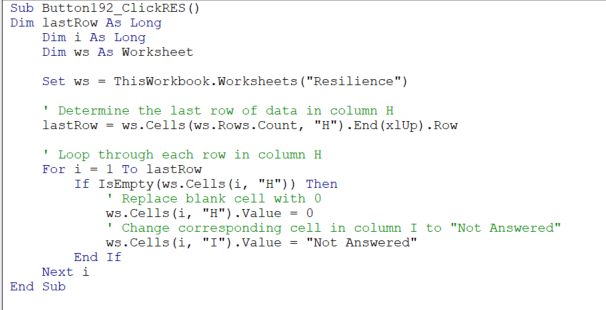


Figure A.4: Programme VBA Résilience

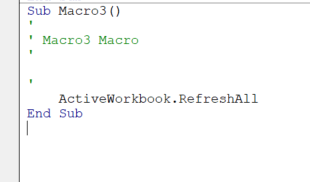


Figure A.5: Programme VBA Dashboard

# **Résumé**

Ce rapport est une synthèse de notre projet de stage au sein de Deloitte Morocco Cyber Center, portant sur le développement d'un toolkit pour la fourniture de services CISO en tant que service. Le rapport est divisé en quatre chapitres clés : présentation de l'entreprise d'accueil, contexte général du projet, étude détaillée du projet et réalisation concrète du projet.

Dans le premier chapitre, nous présentons l'entreprise d'accueil, en soulignant son expertise en matière de cybersécurité et son rôle de leader dans le secteur. Nous avons également présenté les différents piliers disponibles au sein du Deloitte Morocco Cyber Center.

Le deuxième chapitre aborde le contexte général du projet, en expliquant les besoins du marché en matière de CISO as a service et en soulignant les avantages et les défis associés à cette approche. Nous avons également discuté le planning que j’ai suivi durant ma période de stage.

Le troisième chapitre a été consacré à une étude détaillée du projet, où nous avons décrit en profondeur les différentes cas d’utilisation et services pour développer le toolkit. Nous avons abordé la conception de l'approche et du Framework, l'élaboration des questionnaires et des entretiens, et l'évaluation des mesures de sécurité mises en place par le client.

Enfin, dans le quatrième chapitre, nous présentons les réalisations concrètes du projet, notamment l’utilisation du toolkit et du tableau de bord automatisé pour évaluer le niveau de maturité du client en matière de sécurité.

En conclusion, ce rapport de stage témoigne de notre expérience enrichissante dans le développement d'un toolkit pour fournir des services de CISO as a service. Ce projet a été une occasion unique de mettre en pratique nos connaissances en matière de cybersécurité et de contribuer à la protection des informations sensibles des organisations. Les perspectives d'amélioration continue offrent des possibilités intéressantes de répondre aux besoins changeants du marché et de maintenir une protection solide contre les cybermenaces.

# **Abstract**

This report is a summary of our internship project at Deloitte Morocco Cyber Center, involving the development of a toolkit for the provision of CISO services as a service. The report is divided into four key chapters: presentation of the host company, general context of the project, detailed study of the project and concrete realization of the project.

In the first chapter, we introduce the host company, highlighting its expertise in cybersecurity and its leading role in the sector. We also present the various pillars available within the Deloitte Morocco Cyber Center.

The second chapter addresses the general context of the project, explaining the market needs for CISO as a service and highlighting the benefits and challenges associated with this approach. We also discussed the schedule I followed during my internship period.

The third chapter was devoted to a detailed study of the project, where we described in depth the various use cases and services for developing the toolkit. We discussed the design of the approach and framework, the development of questionnaires and interviews, and the evaluation of the security measures implemented by the customer.

Finally, in the fourth chapter, we present the concrete achievements of the project, in particular the use of the toolkit and the automated dashboard to assess the customer's level of security maturity.

In conclusion, this internship report bears witness to our rewarding experience in developing a toolkit to provide CISO as a service. This project was a unique opportunity to put our knowledge of cybersecurity into practice and contribute to the protection of organizations' sensitive information. The prospects for continuous improvement offer exciting opportunities to meet changing market needs and maintain solid protection against cyber threats.