Haute Ecole

ICHEC – ECAM – ISFSC

Enseignement supérieur de type long de niveau universitaire

Comment assurer la sécurité de l'information dans la mise en œuvre d'un outil collaboratif de gestion de laboratoire au sein du groupe Solvay ?

Mémoire présenté par :

Caroline ELOY

Pour l'obtention du diplôme de :

Master en alternance en Business Analyst

Année académique 2020-2021

Promoteur :

Monsieur Alain EJZYN

Boulevard Brand Whitlock 6 - 1150 Bruxelles

Haute Ecole

ICHEC – ECAM – ISFSC

Enseignement supérieur de type long de niveau universitaire

Comment assurer la sécurité de l'information dans la mise en œuvre d'un outil collaboratif de gestion de laboratoire au sein du groupe Solvay ?

Mémoire présenté par :

Caroline ELOY

Pour l'obtention du diplôme de :

Master en alternance en Business Analyst

Année académique 2020-2021

Promoteur :

Monsieur Alain EJZYN

Boulevard Brand Whitlock 6 - 1150 Bruxelles

Remerciements

Je tiens tout d'abord à remercier ma maitre de stage, Madame Véronique Mathieu, manager du département analyse de Bruxelles de m'avoir acceptée en tant que stagiaire au sein de son département. Je tiens également à la remercier pour sa confiance, son expertise, son soutien et sa disponibilité qui m'ont guidée, non seulement durant mon stage mais également tout au long de ce travail.

Je désire également remercier mon promoteur, Monsieur Alain Ejzyn, pour le temps qu'il m'a consacré, pour répondre à mes nombreuses questions. Son aide, son temps, ses recommandations ainsi que son expertise m'ont permis de réaliser au mieux mon mémoire.

Je remercie chacune des personnes qui ont pris le temps de répondre à mes questions lors d'entretiens : Mathieu Fenoll, Xavier Paulus, Guillaume Collard et Hervé Gazio, sans qui la réalisation de ce mémoire n'aurait pas été aussi complète.

Pour terminer, je tiens à remercier mes parents, pour le temps qu'ils ont investi qu'ils m'ont apporté dans la réalisation de ce travail, ainsi que leur soutien qu'ils m'ont apporté tout au long de mes études.

Caroline Eloy

Engagement Anti-Plagiat du Mémoire

« Je soussigné, ELOY, Caroline, 2020-2021, déclare par la présente que le Mémoire ci-joint est exempt de tout plagiat et respecte en tous points le règlement des études en matière d'emprunts, de citations et d'exploitation de sources diverses signé lors de mon inscription à l'ICHEC, ainsi que les instructions et consignes concernant le référencement dans le texte respectant la norme APA, la bibliographie respectant la norme APA, etc. mises à ma disposition sur Moodle.

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

Dans le cadre de ce dépôt en ligne, la signature consiste en l'introduction du mémoire via la plateforme ICHEC-Student.

« We have always operated by imposing on our minds a duty of continuous progress. »

- Ernest Solvay

Table des matières

Liste des tableaux

Liste des figures

Introduction

Voici le moment à la fois tant attendu et tant redouté par les étudiants ; la réalisation du mémoire.

Tant attendu car il représente la fin d'un cycle important et un accomplissement qui ouvre les portes sur le début d'une carrière.

Tant redouté car il correspond à l'élaboration d'un gros travail d'analyse qui peut paraitre complexe et insurmontable tant qu'il est abstrait et qu'on n'y a pas encore mis les pieds de plein fouet. Et puis, l'opportunité m'a été offerte d'accomplir mon stage en alternance dans une entreprise qui a été pour moi une réelle source d'apprentissage : l'entreprise Solvay, et plus précisément le département analyse de Bruxelles.

L'entreprise Solvay est spécialisée dans la chimie et est un acteur majeur dans l'innovation. L'arrivée de sa nouvelle CEO Ilham Kadri en 2018 a amené son lot de changements avec l'objectif de conserver sa première place sur le marché de la chimie. En effet, les évolutions technologiques liées à notre époque, telles que la digitalisation, mais aussi la prise en considération de la sécurité de l'information qui en découle ont fait l'objet d'une attention toute particulière. Bien qu'elle ait pu prendre de justesse le train en marche pour digitaliser ses processus et mettre en place une gestion de sécurité adéquate, la taille de Solvay implique un manque de coordination entre ses sites et ses entités, qui souvent ne sont pas à jour dans les nouveautés adoptées par le groupe.

C'était le cas du département analyse de Bruxelles, qui, lors de la mise en place d'un projet collaboratif entre les différents départements analyse du groupe, s'est vite fait rattraper par ses lacunes en termes de sécurité de l'information. Face à cette problématique réelle vécue par le département dans lequel j'ai pu travailler durant deux années en tant que stagiaire, Véronique Mathieu, manager du département, m'a confié la tâche de l'épauler et de l'aider à apporter des réponses à ces questions : qu'est-ce que cela implique pour le département ? Ces lacunes en matière de sécurité de l'information allaient-elles impacter mon département, et si oui, à quel niveau ? Comment intégrer cette gestion de la sécurité au département ? Le sujet de mon mémoire s'est donc imposé à nous, comme une évidence : « Comment assurer la sécurité de l'information dans la mise en œuvre d'un outil collaboratif de gestion de laboratoire au sein du groupe Solvay ? ».

J'ai rédigé ce mémoire en trois parties : la contextualisation, la mise en œuvre et les recommandations.

La partie de contextualisation correspond à l'état de l'art, soit à une recherche dans la littérature spécifique par rapport au sujet abordé. Dans cette partie, vous trouverez en préambule un premier chapitre sur le cadre général de la sécurité de l'information ; l'importance de sa prise en considération mais également en quoi consiste la sécurité de l'information. J'y aborde ensuite un inventaire non exhaustif des menaces qui pèsent sur la sécurité de l'information ainsi que les impacts que cela peut engendrer sur l'organisation. Nous

ferons ensuite le point sur les enjeux de la sécurité de l'information ainsi que la présentation d'une méthodologie de gestion des incidents. Je finirai par vous présenter les différents acteurs qui peuvent avoir un rôle dans la sécurité de l'information d'une entreprise.

Un second chapitre détaillera une des démarches pouvant être mise en place pour gérer la sécurité de l'information ainsi qu'une méthode de gestion du changement qui peut s'appliquer en parallèle à cette démarche.

Enfin, un dernier chapitre présentera les différentes normes et méthodes d'analyses de risques que la littérature propose en matière de sécurité de l'information.

La deuxième partie de ce travail développe la mise en œuvre pratique des points vus dans le cadre de la contextualisation et basée sur la mission concrète que j'aide à mener au cours de mon stage chez Solvay. Elle débutera par une présentation de l'organisation de l'entreprise Solvay au niveau de sa gouvernance mais également en termes de sécurité de l'information, avec une explication de ce qui était déjà mis en place au sein du groupe. Nous prendrons connaissance de ce qu'est un système de gestion de laboratoire et comment celui-ci a été mis en place au sein de Solvay. Ces informations permettent de mieux comprendre les enjeux de la mise en place d'un outil collaboratif au sein du département analyse, mais aussi d'en comprendre le fonctionnement et l'utilité.

C'est sur base de ces éléments que j'ai été amenée à élaborer une solution de sécurité de l'information adéquate au département mais également à réaliser une analyse de risques relative à l'utilisation de l'outil au sein de ce département.

Pour conclure, cette analyse de risques nous amènera à la dernière partie de ce mémoire, soit une recommandation en matière de mesures de sécurité à appliquer pour protéger le département d'éventuels incidents. En effet, l'élaboration d'une analyse de risques mène à des recommandations ciblées, que nous évaluerons dans cette partie. Ensuite, une élaboration de gestion du changement en lien avec le projet sera présentée.

Présentation de l'entreprise

L'entreprise Solvay (Solvay, 2021, *History*) a été créée il y a plus de 150 ans. A ses débuts, l'entreprise Solvay était exclusivement une entreprise de production de carbonate de sodium. C'est suite à la crise de l'huile de 1973, que Solvay élargit sa sphère au secteur pharmaceutique et s'ouvre aux sciences de la vie, soit la biochimie. En 2009, Solvay vend ses activités pharmaceutiques au groupe Abbott, ce qui lui permet en 2010 de faire une OPA afin de racheter l'entreprise Rhodia. Cet achat va permettre à Solvay de devenir leader mondial sur le marché de la chimie (Solvay, 2021, *History*). Depuis 2018, Ilham Kadri assure le poste de CEO de l'entreprise Solvay. Elle est la première femme CEO du groupe (Solvay, 2021, *History*).

Le groupe Solvay est une SA internationale, leader sur le marché de la chimie. Son chiffre d'affaires s'élevait à 8,9 milliards d'euro en 2020 (Rapport Annuel Intégré, 2020, p. 8). Elle emploie un peu plus de 23.000 personnes et est présente dans 64 pays (Rapport Annuel Intégré, 2020, p. 8). Solvay possède à son actif 110 sites industriels et 20 centres de Recherche et Innovation répartis dans le monde (Amérique du Nord, Amérique du Sud, Europe, Asie, …).

L'entreprise est active, de manière directe ou indirecte, sur plusieurs secteurs d'activité (Solvay, 2021, *Solutions by market*), tels que l'aéronautique et l'automobile, l'agroalimentaire, le bâtiment et la construction, les biens de consommation et la santé, les appareils électriques et électroniques, l'énergie et l'environnement et les applications industrielles. C'est une entreprise spécialisée dans les matériaux avancés et la chimie de spécialité. Orientée vers l'innovation et la durabilité, elle a pour but de répondre aux grands enjeux de la société (Solvay, 2021, *What is Solvay ?*).

En Belgique, Solvay produit des peroxydes, des polymères spéciaux et est active dans l'extraction de calcaire (Solvay, 2021, *Solvay en Belgique*).

Partie 1 : Contextualisation

La sécurité de l'information est au cœur de l'actualité depuis plusieurs mois, évoquant des cyberattaques à l'encontre d'entreprises mais également de particuliers. Les mots phishing, malware, ransomware sont souvent évoqués mais surtout incompréhensibles et trop techniques pour susciter l'adhésion du grand public face à la gravité de la situation. Et pourtant, la Belgique compte parmi les pays les plus touchés par des cyberattaques (Le Soir, 25 mars 2021), c'est donc essentiel de s'intéresser de près à ce que représente la sécurité de l'information.

Dans le monde de l'entreprise, l'utilisation du cloud et la démocratisation de l'utilisation des applications web exposent les organisations aux cyberattaques, devenant plus vulnérables et plus facilement attaquables, grâce à l'ouverture à de nouveaux moyens d'entrées pour les cybercriminels. Face à tant de menaces et à la dépendance grandissante à laquelle nous sommes confrontés, l'investissement dans une solution de sécurité de l'information n'est plus une option (Ejzyn et Van den Berghe, 2018).

Investir dans la sécurité de l'information implique un changement des habitudes, pas toujours apprécié par les usagers. Cela implique donc une gestion de projet alignée avec un plan de gestion du changement.

Nous l'avons compris, la sécurité de l'information est importante. Cette première partie de mon mémoire est divisée en trois chapitres, qui permettent de contextualiser et de mieux comprendre ce qu'est la sécurité de l'information. Le premier chapitre est consacré au cadre général de la sécurité de l'information. Le second chapitre établit une démarche de gestion de sécurité de l'information et le dernier chapitre présente les différentes normes et méthodes d'analyse de risques adaptés à la gestion d'un système d'information.

1. Cadre général de la sécurité de l'information

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

Avant de définir ce qu'est la sécurité de l'information, il est important de définir ce que sont l'information et la sécurité de manière distincte.

- La sécurité sociale belge définit l'**information** comme étant « une ressource qui, comme toute autre ressource importante, doit être protégée/sécurisée adéquatement » (Sécurité sociale, 2017, p. 5).
- La **sécurité**, au sens large, permet d'éviter des menaces.

La **sécurité de l'information** se définit comme étant la « capacité de l'organisation à garantir la confidentialité, l'intégrité et la disponibilité de l'information et des processus qui ont une valeur pour l'entreprise » (Ejzyn et Van den Berghe, 2018, p. 18). Elle n'est pas à confondre avec la cybersécurité. En effet, alors que la sécurité de l'information concerne tous les

systèmes informatiques – comme par exemple le matériel utilisé pour stocker l'information –, la cybersécurité ne concerne que les systèmes informatiques connectés, que ce soit à internet ou en réseau – soit les outils utilisés pour échanger des données – et permet de se protéger face à la cybercriminalité.

On peut donc résumer la sécurité de l'information à tous les moyens mis en œuvre dans le but de protéger les ressources d'une organisation de la manière la plus adéquate afin d'éviter les risques encourus par la non-sécurisation de celle-ci. Même si l'objectif est de sécuriser l'information, il est important de garder à l'esprit que c'est le système d'information qui doit être sécurisé pour garantir la sécurité de l'information qu'il contient (Ejzyn et Van den Berghe, 2018).

1.1.1. Les principes fondamentaux de la sécurité de l'information

Trois principes fondamentaux sont systématiquement mentionnés par les experts lorsqu'il s'agit de sécurité de l'information, ils les définissent de manière similaire. Ces trois principes doivent être respectés lors de la mise en place d'un système de l'information sécurisé (Ejzyn et Van den Berghe, 2018). C'est à l'entreprise de déterminer l'étendue des règles fixées pour garantir la sécurité de l'information tout en respectant ces principes.

1. La **disponibilité de l'information** : l'entreprise s'assure que l'information reste accessible et disponible pour les personnes compétentes en son sein.
2. Il est important de veiller à couvrir l'**intégrité de l'information** afin de garantir qu'elle ne puisse être modifiée ou supprimée que par les personnes compétentes, et continue de constituer la réalité de ce qu'elle représente.
3. Un des principes les plus connus est celui de la **confidentialité de l'information**, impliquant de garantir le respect des règles de diffusion de ladite information. Il faut déterminer les personnes et systèmes autorisés à accéder à ces informations confidentielles. Cela est d'autant plus important lorsqu'il s'agit d'information de valeur intrinsèque.

Par ailleurs, selon Cartau (2018), le principe de preuve de l'information est également à prendre en compte pour garantir la sécurité d'une information et de son système. Cela implique la traçabilité des actions réalisées sur l'information, et elle se décline sous quatre formes de preuves :

- La non-répudiation de l'information qui va attester que l'information a été émise par l'émetteur désigné et bien réceptionnée par le destinataire désigné. Cela peut se faire sous forme d'accusé de réception.
- L'audit de l'information qui permet de mettre en place une traçabilité des actions exécutées par les personnes compétentes sur l'information.
- La trace de l'information qui va permettre le suivi des opérations réalisées, il s'agit de traces techniques, connues sous le terme de « logs ».
- L'imputabilité de l'information qui permet d'attribuer une action à un utilisateur.

D'autre part, la plateforme fédérale belge eHealth (2021) renforce l'idée d'importance de l'ensemble des principes précités, en présentant directement six principes à prendre en

compte : la confidentialité, la disponibilité, l'intégrité, l'authenticité qui rejoint le principe d'imputabilité, l'irréfutabilité qui rejoint le principe de non-répudiation et l'auditabilité de l'information.

1.1.2. Les menaces de la sécurité de l'information

Une menace intervient lorsque le système informatique présente une ou plusieurs vulnérabilité(s), qu'elles aient été sécurisées ou non. Plusieurs techniques d'attaque existent à l'encontre des nombreuses menaces qui pèsent sur les systèmes d'informations. Chaque menace peut avoir un impact sur l'entreprise et sur son business. Il est donc indispensable d'être prévoyant quant à ces menaces afin de se protéger et d'éviter d'éventuelles attaques, car celles-ci peuvent potentiellement impacter le business et engendrer des pertes, que ce soit au niveau des clients, du chiffre d'affaires ou de l'avantage concurrentiel de l'entreprise. Pour qu'un système informatique soit sécurisé, il faut garantir la confidentialité, l'intégrité et la disponibilité de l'information.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI, 2021) présente les quatre principales menaces qui pèsent sur la sécurité de l'information : la déstabilisation, l'espionnage, le sabotage et la cybercriminalité. Les voici détaillées ci-dessous.

a. La déstabilisation

Trois attaques sont préconisées lorsque l'objectif est la déstabilisation :

- La **saturation** (ou également appelé attaque par déni de service) a pour but de saturer un service web pour qu'il ne soit plus atteignable par les utilisateurs.
- La **défiguration** est utilisée souvent dans des cas de revendication : le but de l'attaquant est d'infiltrer un service web pour en modifier le contenu en tirant avantage des vulnérabilités du système attaqué.
- L'**exfiltration et divulgation des données** est une attaque utilisée pour déstabiliser mais peut également être utilisée à des fins cybercriminelles, abordées ci-dessous. Le but de l'attaquant est, dans ce cas-ci, de prouver le manque de sécurité du système de sa victime en infiltrant son réseau et en dérobant ses données confidentielles pour les divulguer.

b. L'espionnage

L'espionnage est souvent utilisé à des fins économiques et scientifiques. Cette menace est double car elle peut s'exercer à distance ou de manière directe, c'est-à-dire par le biais d'une réelle personne s'infiltrant dans l'entreprise de manière légale et déguisée, en se faisant engager par exemple, en interne ou en consultance. Elle a donc accès aux informations sensibles de façon légitime. L'entreprise peut donc mettre des années avant de se rendre compte qu'elle est victime d'une attaque d'espionnage.

L'espionnage peut également s'opérer via une cyberattaque, en utilisant des logiciels malveillants ou en introduisant des virus, de type cheval de Troie par exemple. Ces différentes attaques seront abordées plus bas dans ce paragraphe.

Cependant, certaines attaques d'espionnage à des fins économiques ou scientifiques sont typiques à certains secteurs (ANSSI, 2021) :

- L'**attaque par point d'eau** qui consiste à infecter un site internet utilisé par des membres de l'entreprise visée. En accédant à ce site, les membres de l'entreprise sont piégés par les attaquants qui vont pouvoir accéder aux machines utilisées pour accéder au site internet.
- L'**attaque par hameçonnage ciblé** opère généralement par le biais d'envoi d'emails dans lequel la cible est invitée à télécharger une pièce jointe ou à se rendre sur un site internet par le biais d'un lien. Suite à l'une de ces actions, l'attaquant va avoir accès à la machine utilisée et va tenter d'y dérober des codes d'accès et des droits d'administrateurs afin d'avoir accès à l'information recherchée.

c. Le sabotage

Comme son nom l'indique, il s'agit d'une attaque qui a pour but de saboter un système informatique afin de le rendre inutilisable.

d. La cybercriminalité

La cybercriminalité désigne « toutes les activités illégales menées à l'aide de la technologie » (Avast, 2021). D'après le rapport d'IBM Security X-Force (2021), l'Europe a été la plus ciblée en matière de cyberattaque en 2020 dont 21% étaient des ransomware et 16% étaient des attaques internes (IBM Security X-Force Threat Intelligence Index, 2021, p. 29). Il existe plusieurs types d'attaques informatiques, et toujours d'après le rapport, les trois principales en 2020 étaient les suivantes :

Tableau 1 : les trois principales attaques informatiques de 2020

Le ransomware	Aussi appelé « rançongiciel », il s'agit d'un logiciel qui va prendre possession d'un ordinateur et qui va menacer de supprimer toutes ses données en échange d'une rançon. Ce sont des attaques ciblées, qui s'adaptent en fonction de leur cible. 23% des attaques sont des ransomware, alors qu'en 2019, cela représentait 20% des attaques (IBM Security X-Force Threat Intelligence Index, 2021, p. 8).
Le vol de données	Cela représente 13% des attaques informatiques survenues en 2020, contre 5% en 2019, soit une hausse de 160% (IBM Security X-Force Threat Intelligence Index, 2021, p. 11)
L'accès au serveur	Une personne malveillante réussi à accéder au serveur de diverses manières (par un vol d'identifiants ou suite à une vulnérabilité dans le système par exemple) Cela représente 10% des attaques informatiques en 2020, contre 3% en 2019, ce qui représente une hausse de 233% en un an ((IBM Security X-Force Threat Intelligence Index, 2021, p. 8).

S'il s'agit des trois attaques principales présentées par le rapport d'IBM (2021), ce ne sont pas les seules mentionnées. En effet, on peut également parler de :

- Business Email Compromise (BEC) : il s'agit d'une attaque qui consiste à usurper l'identité d'une personne de l'entreprise, tel qu'un directeur, un fournisseur ou un client, dans le but de demander un paiement commercial. Elle peut être utilisée à des fins financières mais également dans le but de voler des données personnelles (Weststarbank, 2021).
- Remote Access Trojan (RAT) : il s'agit d'une attaque de type « cheval de Troie ». Il s'agit d'un logiciel qui peut être envoyé via un courrier électronique sous forme d'un fichier annexe ou de lien. Lorsque le logiciel s'installe sur votre équipement, cela permet l'accès total à celui-ci (CaixaBank, 2021).
- Mauvaise configuration : il s'agit d'une attaque qui cherche les vulnérabilités dues à une mauvaise configuration d'un système d'information.

Ces attaques peuvent s'opérer via différents vecteurs, dont les trois principaux sont les suivants (IBM Security X-Force Threat Intelligence Index, 2021) :

Tableau 2 : les trois principaux vecteurs d'attaques informatiques en 2020

Scan-and-exploit	Il s'agit de scanner les mesures de sécurité mises en place sur un système d'information et d'en exploiter les vulnérabilités pour accéder aux informations. Cela peut se faire via les infrastructures internes mais également externes à une organisation, tel qu'un outil fournit par un fournisseur tiers par exemple (Jumpsec. (2021). 2 avril 2021). En 2020, ce vecteur représente 35% des attaques informatiques alors qu'il ne représentait que 30% en 2019 (IBM Security X-Force Threat Intelligence Index, 2021, p. 13).
Phishing	Aussi appelé « Hameçonnage ». Cette méthode fonctionne souvent via emails, dans lequel une personne mal intentionnée va se faire passer pour une organisation légitime connue par l'entreprise attaquée. L'email va inciter le destinataire à cliquer sur un lien URL ou à télécharger une pièce jointe, permettant à l'attaquant de dérober des informations confidentielles (CNIL. (s.d.). 24 mars 2021). En 2020, le phishing représente 33% des vecteurs utilisés dans le but de réaliser une attaque informatique, contre 31% en 2019 (IBM Security X-Force Threat Intelligence Index, 2021, p. 7). Le phishing n'est pas à confondre avec les spams qui sont des courriers certes indésirables mais qui ne représentent pas de menace pour une organisation.
Vols d'identifiants	Il s'agit de réaliser une attaque informatique en ayant dérobé les identifiants d'un employé ou d'un tiers de l'entreprise attaquée ; Ce vecteur représente 18% des attaques informatiques en 2020. Il est en diminution depuis 2019 au profit du vecteur « scan-and-exploit » précité (IBM Security X-Force Threat Intelligence Index, 2021, p. 13).

Bien que ces menaces n'impliquent pas directement l'utilisateur, il faut garder en tête que ces attaques sont possibles le plus souvent à cause des utilisateurs qui ne sont pas forcément conscients du risque encouru. 95% des cyberattaques aboutissent suite à une erreur humaine

(Cybint, 2021). Sans oublier que même si une attaque est réalisée sur une seule machine, cela suffit pour infiltrer l'ensemble de son parc informatique (Ejzyn et Van den Berghe, 2018).

1.1.3. Les impacts de la sécurité de l'information

Les entreprises victimes de ces attaquent peuvent subir différents impacts (Ejzyn et Van den Berghe, 2018) :

1. Un **impact financier** ;

Une attaque visant le système de gestion de commande d'une entreprise – ou tout autre outil de gestion de l'entreprise –, peut impacter directement son activité, et ainsi engendrer une perte financière importante sur le long terme. De plus, si l'attaque a endommagé le système, de nombreux coûts peuvent en découler, tels que des coûts de réparation et de maintenance. Si l'attaque est de type rançongiciel, une rançon devra être payée par l'entreprise si elle souhaite récupérer les informations qui lui ont été dérobées.

Par la suite, l'entreprise sera dans l'éventualité de mettre en place des mesures de sécurité afin d'éviter une éventuelle attaque du même type, ce qui engendre évidemment des coûts, qui certes doivent être dépensés, mais si ces mesures avaient été mises en place dès le départ, les attaques n'auraient probablement pas eu lieu.

2. Un **impact sur ses missions** ;

Si une attaque vise et endommage un outil de gestion de commande, celles-ci prendront du retard et l'entreprise ne sera plus en mesure d'assurer ses missions vis-à-vis de ses parties prenantes.

3. Un **impact juridique** ;

Une attaque peut impacter les différents contrats existant entre les parties prenantes, se résultant par un non-paiement de solde, une annulation de livraison, … Dans le cas où le système de gestion des finances est impacté, des sanctions administratives fiscales peuvent être administrées.

L'entreprise Picanol est un exemple qui rassemble ces trois impacts. Victime d'une cyberattaque de type rançongiciel (cf. supra p. 7) en janvier 2020 (RTBF, 14/01/2020), elle a été contrainte d'arrêter sa production pendant une semaine. Le système d'information ainsi que la majorité de sa production informatisée ont été attaqués. L'entreprise s'attend à un impact financier d'un million d'euros (Le soir, 31/01/2020).

1. Un **impact sur la réputation** ;

Certaines attaques sont réalisées dans l'unique but de démontrer les failles de sécurité d'une entreprise. Cela peut avoir un effet néfaste sur la confiance accordée par les clients qui constatent que l'entreprise avec laquelle ils travaillent ne sécurise pas ses actifs.

C'est le cas de l'entreprise britannique de télécom TalkTalk, victime de trois cyberattaques en l'espace de 12 mois. C'est en octobre 2015, lorsque la troisième cyberattaque est réalisée par des adolescents que l'entreprise va sombrer, révélant une réelle faiblesse des systèmes de sécurité de l'entreprise. Suite à ces attaques et aux nombreux témoignages sur les réseaux sociaux, l'entreprise TalkTalk aurait perdu 7% (Les éclaireurs de la com', 8/04/2019) de ses clients, soit 300 000 personnes, pour passer à la concurrence.

1.2. Les enjeux de la sécurité de l'information

Ces menaces et leurs impacts mettent en avant deux grands enjeux généraux auxquels une entreprise peut faire face du point de vue sécurité de l'information, également soulignés par Cartau (2018) : les enjeux techniques mais également les enjeux liés aux comportements humains. Les enjeux présentés dans cette section sont non-exhaustifs.

1.2.1. Les enjeux techniques

a. *D'un point de vue infrastructure*

La sécurité des réseaux

Dans un premier temps, il est impératif de sécuriser le réseau dans son ensemble. Comme on a pu le constater, de nombreuses menaces pèsent et peuvent s'infiltrer par le biais du réseau auquel la machine attaquée est connectée (Ejzyn et Van den Berghe, 2018).

Même si le réseau ne contient, ni ne traite l'information, c'est par celui-ci qu'elle transite. Il s'agit donc d'une voie d'accès favorable aux cyberattaques. Voici un schéma qui permettra de mieux comprendre le mécanisme d'un réseau :

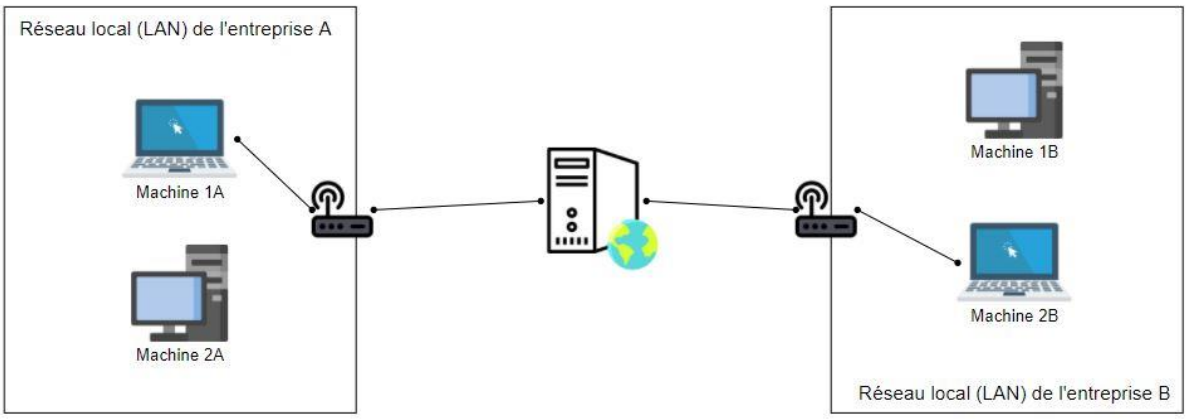

Figure 1 : Schéma d'une communication de bout en bout entre deux réseaux LAN
Source des images : https://www.flaticon.com/

Sur ce schéma, on peut y voir une communication entre deux machines de deux réseaux LAN différents. Un réseau LAN est un réseau local qui va connecter entre eux tous les équipements d'une même zone, comme par exemple les équipements d'un même bâtiment. Il est important de souligner que les équipements ne signifient pas uniquement les ordinateurs, mais tout équipement connecté, soit les imprimantes, les tablettes, …

Afin de connecter deux réseaux pour leur permettre de communiquer entre eux, ces réseaux locaux doivent passer par un réseau plus étendu, qui s'appelle réseau WAN, dont le plus connu est internet. Lorsque la Machine 1A va vouloir envoyer une information à la Machine 2B, elle va envoyer ce qu'on appelle un « paquet » dans lequel l'information va transiter.

Internet permet la transition de paquets entre deux réseaux, et ce paquet ne va pas suivre le même chemin entre son expéditeur et son destinataire. C'est lors de cette transmission que peut survenir une cyberattaque pour tenter d'intercepter ce paquet.

Pour s'en prémunir, il est donc impératif de protéger le réseau via lequel les paquets transitent. Et cela peut se faire de plusieurs manières :

- En cryptant les données qui transitent (l'utilisation de site web suivant le protocole HTTPS permet cela).
- En utilisant un VPN, qui permet de créer un service de réseau privé ; cela offre la possibilité de sécuriser plusieurs réseaux locaux entre eux et de garantir la sécurité des transmissions de données entre ces réseaux.
- En utilisant des pare-feu (ou Wireframe) qui vont permettre de contrôler les données entrantes et sortantes d'un réseau. Il est placé entre le réseau de l'entreprise et le réseau d'internet. C'est un équipement indispensable pour des entreprises qui doivent communiquer avec d'autres réseaux externes. Cela permet de se protéger des éventuelles menaces précitées (cf. supra p. 6).

La sécurité physique et environnementale

Comme expliqué, même si le réseau ne traite pas l'information à sécuriser, cela n'empêche pas qu'il subisse des attaques. Il en va de même pour les infrastructures physiques situées sur le réseau ainsi que leur environnement (Ejzyn et Van den Berghe, 2018).

En effet, il est tout aussi important de protéger et d'adapter l'infrastructure physique qui contient les divers équipements de manière à ce que le système d'information soit protégé contre tous risques éventuels.

Mais ce n'est pas tout, il est également important de protéger l'environnement de cette infrastructure physique. L'évolution de la digitalisation a permis de mettre en place des équipements modernes de protection d'environnement, connectés et gérés par les réseaux, tels que des systèmes de surveillance et de gestion des accès d'un bâtiment. Cela sort du champ d'application de ce travail, mais cela n'en retire pas le lien qu'il y a entre la sécurité physique et la sécurité de l'information.

b. D'un point de vue logiciel

Le cloud

En pleine expansion, le cloud est devenu un enjeu majeur en termes de sécurité de l'information. En effet, le cloud permet de stocker l'information et d'y avoir accès par internet au-delà des frontières d'un réseau local. L'utilisation du cloud permet aux entreprises

d'externaliser leurs systèmes d'information, ce qui, en cette période de télétravail imposée, ne peut plus être perçu comme un élément superflu (Protime. (2020). 12 avril 2021).

Une entreprise peut créer ses propres serveurs cloud et les intégrer à son infrastructure mais cela représente un coût. C'est pourquoi il est possible de faire appel à un fournisseur de cloud (les plus connus étant Google, Microsoft ou encore Amazon Web Service). En fonction des besoins de l'entreprise face à ce service cloud, trois modèles de cloud listés ci-dessous sont proposés sur le marché (voir ANNEXE 1 : Les modèles de cloud) :

- Le modèle SaaS (« Software as a service ») propose une externalisation du matériel – tels que les serveurs et le réseau de sauvegarde –, des logiciels et d'une partie des données dans le cloud. Tout cela est sous la responsabilité du fournisseur.
- Le modèle PaaS (« Plateforme as a service ») propose une externalisation du matériel et du système d'exploitation qui sont sous la responsabilité du fournisseur. C'est à l'entreprise de prendre en charge l'installation du logiciel d'application et de gérer ses données.
- Le modèle IaaS (« Infrastructure as a service ») propose d'externaliser uniquement le matériel qui est sous la responsabilité du fournisseur. La responsabilité des données, du logiciel d'application et du système d'exploitation revient à l'entreprise.

Bien souvent, l'utilisation du cloud implique une dépendance auprès d'un fournisseur, il faut donc garder en tête que l'entreprise peut être impactée dans le cas où le fournisseur est sujet à une menace.

L'utilisation du cloud a également fait émerger les applications web, devenues un nouvel enjeu pour les entreprises. Par définition, l'application web est une plateforme qui ne doit pas être installée sur une machine car elle est directement accessible depuis internet. Il peut s'agir d'un système de messagerie mais également d'un système de gestion de contenus de tous genres (Scalair, 2020).

Les applications web peuvent contenir des informations cruciales pour l'entreprise dont la sécurité est indispensable. C'est pourquoi les applications web sont sujettes également aux nombreuses menaces précitées (cf. supra p. 6). Souvent proposées par des fournisseurs, c'est à l'entreprise de se renseigner sur les mesures de sécurité appliquées par les fournisseurs concernant l'application web utilisée. L'entreprise sera en effet directement impactée en cas d'incident subi par le fournisseur.

La gestion des accès aux systèmes d'information

Comme expliqué, les données sont stockées sur des équipements informatiques qui doivent être sécurisés pour garantir la confidentialité, l'intégrité et la disponibilité de l'information. Pour cela, la gestion des accès est une des premières mesures à mettre en place. Cette gestion est conséquente et implique de la rigueur, elle doit être systématique, surtout avec l'expansion des attaques de type vol de données (cf. supra p. 7). Il s'agit d'une gestion qui s'exerce en trois étapes (Ejzyn et Van den Berghe, 2018) :

- L'identification : il s'agit de déclarer qui est l'utilisateur (via son nom, un identifiant, une adresse e-mail ou même un pseudonyme).
- L'authentification : elle se fait par utilisation d'un mot de passe (ou même une empreinte) qui va prouver l'authenticité de l'identification de l'utilisateur.
- L'autorisation : suite aux deux précédentes étapes, le système va pouvoir accorder un accès aux informations qu'il contient. Il existe plusieurs types d'autorisation : en lecture seule, en commentaire, en écriture, ou même une autorisation d'ajouter, modifier ou supprimer une donnée.

Il existe plusieurs modèles permettant de gérer les accès aux ressources :

Tableau 3 : les modèles de gestion des accès aux ressources

Le **DAC** (« Discretionary Access Control »)	Dans ce cas-ci, c'est le propriétaire de la ressource qui va gérer la gestion des accès de celle-ci.
Le **RBAC** (« Role-Based Access Control »)	Dans ce cas-ci, l'utilisateur se voit attribuer un rôle qui va déterminer l'accès qu'il aura aux différentes ressources. Un utilisateur peut avoir plusieurs rôles et vice versa.
Le **MAC** (« Mandatory Access Control »)	Dans ce cas-ci, des niveaux de sécurité sont associés aux différentes ressources. Chaque niveau possède ses propres règles d'accès aux ressources.

Il existe également une technique de gestion des identités (Ejzyn et Van den Berghe, 2018), plus connue sous le terme IAM (« Identity and Access Management »), qui permet de gérer les comptes et les droits d'accès des différents sous-systèmes de l'entreprise. Il est cependant possible de mettre en place des systèmes d'authentification uniques, ce qui signifie qu'un seul identifiant permettra d'accéder à divers sous-systèmes d'une même entreprise, comme le permettent les systèmes SSO (« Single Sign-on »).

La gestion des logs

Une autre manière de prévenir les fraudes de son système d'information est la mise en place d'une gestion des logs. Un log est un « fichier informatique utilisé pour l'exploitation d'un serveur d'hébergement. Ce fichier conserve la trace de toutes les requêtes qui ont été adressées à ce serveur » (eMarketing.fr, 2021, *Log (Fichier)*). Il permet de tracer toutes activités effectuées par un utilisateur, et donc de récolter les différentes informations qu'il a pu consulter, le moment auquel il y a accédé et le temps qu'il est resté connecté.

La gestion des logs permet d'obtenir un suivi précis des activités du système d'information et est très utile en cas d'incident car elle permet de détecter facilement et rapidement sa source. Dans la plupart des systèmes d'information, les logs sont conservés 24h. S'il est pertinent pour l'entreprise de les conserver afin d'assurer la sécurité de son système d'information, alors il faudra mettre en place une gestion des logs réglementée. Cette gestion des logs se fait en quatre étapes (Logpoint, 2020, *Guide de la gestion des logs et de l'importance de la journalisation*) :

1. Faire une collecte des logs : on peut récupérer soi-même les logs ou mettre en place un processus qui va les collecter automatiquement.

2. Faire une collecte centralisée des logs : il va de soi que les logs collectés sont centralisés et non éparpillés dans plusieurs fichiers différents. Certaines plateformes cloud proposent dans leur solution une gestion des logs.
3. Stocker, conserver et faire des rotations des logs : c'est à l'organisation de décider de la durée de stockage, des raisons de conservation des logs et de la conformité de cette conservation.
4. Choisir la bonne solution de stockage : il est évidemment important de bien choisir le lieu de stockage des logs, pour éviter que quiconque ne puisse y avoir accès et ne puisse s'en servir.

Bien que cette gestion des logs permette d'identifier une attaque par accès ou de déterminer l'origine d'un quelconque incident, il faut faire attention aux données impliquées par leur conservation. En effet, les logs retracent les activités d'un utilisateur, cela peut donc concerner des données à caractère personnel, il faut donc les traiter conformément au règlement général sur la protection des données (RGPD). Il est impératif d'informer les utilisateurs sur le traitement de leurs données, mais également de déterminer un cadre de traitement, qui ne devra pas être dépassé (CNIL, (s.d.), *Sécurité : tracer les accès et gérer les incidents*).

c. *D'un point de vue matériel*

La montée du télétravail a changé la manière dont on sécurise les systèmes d'information. Le fait de pouvoir accéder aux informations dont on a besoin depuis le cloud, peut pousser certains employés à favoriser le télétravail, qui permet de gagner du temps, notamment en évitant les trajets et y afférant le trafic par exemple.

Cela implique évidemment une gestion de sécurité du matériel utilisé. Certaines entreprises mettent à disposition de leurs employés du matériel, ce qui permet à l'entreprise de gérer notamment l'aspect sécurité de ceux-ci en y ajoutant des possibilités de gestion uniquement accessibles par les administrateurs qui en ont le droit.

D'autres entreprises permettent à leurs employés d'utiliser leur propre matériel. Cette pratique est connue sous l'appellation BYOD (« Bring your own device »), et permet aux employés d'avoir une utilisation personnelle mais également professionnelle de leur matériel. Afin de rendre cela possible, il est indispensable de mettre en place des solutions sécurisées permettant le travail à distance sur du matériel ne présentant peut-être pas la sécurité imposée par la politique de sécurité de l'entreprise. C'est donc un défi pour celle-ci de déterminer si oui ou non la pratique BYOD peut être implémentée au sein de l'organisation.

1.2.2. Les enjeux humains

Malgré les nombreux enjeux techniques évoqués, l'enjeu le plus souvent mis en cause dans la sécurité de l'information est l'enjeu humain. En effet, s'il n'est pas pris en compte, on risque de rencontrer un grand nombre de problèmes de sécurité (Ejzyn et Van den Berghe, 2018). Dans le cas des enjeux humains, on peut rencontrer deux problèmes ; l'erreur humaine et les actes de malveillances.

Certes « l'erreur est humaine », mais elle peut être évitée. Une erreur humaine peut survenir suite à une mauvaise manipulation, une inadvertance lors de la réception d'un e-mail frauduleux, le fait de se faire voler son matériel laissé sans surveillance. C'est pourquoi il est indispensable d'impliquer les utilisateurs proactivement dans la sécurité, afin de les conscientiser et de les responsabiliser en leur apportant toutes formations nécessaires à cet apprentissage. Une des portes d'entrées favorites des attaquants est le courrier électronique, car elle est la plus ciblée (cf. supra p. 8). Une formation sur les menaces qui pèsent sur les e-mails est de nos jours indispensable.

D'autre part, un utilisateur peut réaliser une erreur de manière volontaire, suite par exemple à un licenciement ou une envie de nuire.

1.3. La gestion des incidents

Même si on est conscient des menaces qui pèsent sur la sécurité de l'information et qu'on a mis en place des mesures liées aux enjeux de la sécurité, certains incidents peuvent quand même survenir. Il est donc judicieux de mettre en place un processus de gestion des incidents, qui permettra à l'entreprise de réagir rapidement et de manière efficace si un incident venait à se produire.

Ejzyn et Van den Berghe (2018) proposent un plan de gestion des incidents clair et complet, similaire à ceux proposés par le Centre for Cyber Security Belgium et par le Clusif – association française de référence de la sécurité numérique. Je vais donc reprendre dans ce chapitre la structure du plan de gestion.

Une gestion des incidents permet de mettre en place un plan de réponse aux incidents. Ceci permet aux acteurs de réagir rapidement pour récupérer le système endommagé dans les meilleurs délais. C'est un processus qui se base sur le système d'amélioration continue et qui impose donc une révision à chaque incident afin d'améliorer constamment son plan de réponse.

1.3.1. Se préparer aux incidents

La première étape est de se préparer aux éventuels incidents qui pourraient survenir et se réalise en trois phases. Premièrement, l'organisation doit définir les priorités de réparation en cas d'incident, en prenant connaissance des différents actifs essentiels et de support du système et d'en indiquer les priorités de récupération lors de la mise en application du plan de réponse. Il est important de désigner une équipe projet qui s'occupera de faire évoluer le plan de réponse aux incidents.

La deuxième phase consiste à définir une équipe et les rôles de chacun. Il faut déterminer les différents acteurs qui seront impliqués dans la gestion des incidents en déterminant leurs rôles et responsabilités respectifs. Cela permet de mettre en action rapidement une équipe projet lorsqu'un incident surviendra.

Pour finir, il faudra assurer une transmission ciblée des informations en établissant une liste des différentes personnes à contacter lors de la survenance d'un incident ainsi que la liste des

informations à leur partager. Le responsable du département ne doit pas recevoir les mêmes informations que l'équipe en charge de gérer les incidents, par exemple, il sera pertinent de prévenir le responsable de département qu'un incident a eu lieu, mais il faudra communiquer à l'équipe de gestion des incidents des détails plus spécifiques sur la nature de l'incident.

1.3.2. Détecter un incident

On peut détecter un incident de plusieurs façons :

- Si les utilisateurs ont été formés et conscientisés sur les différents incidents possibles, ceux-ci entreront directement en contact avec leur référent sécurité ;
- Certains outils automatiques de détection d'incidents peuvent être mis en place.

Il faudra ensuite déterminer le type d'incident qui est survenu car cela va impacter la manière dont on va le traiter : s'agit-il d'une attaque, d'une mauvaise manipulation d'un utilisateur ou d'un élément extérieur tel qu'un incendie, une inondation ?

N.B. : En cas d'attaque, il est important de créer un dossier afin d'éventuellement demander réparation par voie judiciaire, mais il est important de garder à l'esprit que cela engendrera de longues procédures de collecte de preuves. Ces procédures auront un impact sur la disponibilité de l'information étant donné que l'outil endommagé restera inutilisable le temps de celles-ci.

1.3.3. Traiter l'incident

Lorsque l'incident est détecté et identifié, il est temps de le traiter, et cela se fait en deux étapes :

- Isoler l'incident afin d'éviter qu'il se répande et qu'il provoque des répercutions plus importantes que celles déjà causées.
- Éradiquer l'incident en supprimant tout ce qui y est associé, comme des comptes utilisateurs piratés par exemple, ce qui nécessite des compétences techniques qui dépendent de la nature de l'incident.

1.3.4. Reprendre les activités

Une fois l'incident éradiqué, il faudra restaurer le système ainsi que les données dans le meilleur état possible. Dans le cas où l'incident a un impact sur la disponibilité du système, cela va également impacter le niveau de service offert, il faudra donc se charger de contacter les différentes parties prenantes impactées.

1.3.5. Tirer les enseignements

Il s'agit de profiter d'un incident pour améliorer la manière dont on l'a traité. Il faut donc revoir la manière dont l'incident a été géré, dans le but d'améliorer ce processus et de mettre en place un plan de réponse plus ciblé si un autre incident survient.

Il faudra également chiffrer les coûts liés à l'incident. Ces coûts représentent ce qui est relatif à la récupération du système mais également ce qu'a engendré indirectement l'incident, tel que l'indisponibilité du système et la dégradation éventuelle de l'image de l'entreprise.

Dans certains cas, un incident peut révéler une vulnérabilité du système. Il faudra donc déterminer des mesures et des actions à mettre en place pour éradiquer ces vulnérabilités.

1.4. Les acteurs de la sécurité de l'information

On l'a vu à plusieurs reprises, de nombreux acteurs interagissent dans le système de sécurité de l'information. On peut diviser les acteurs de la sécurité en quatre catégories :

- Les utilisateurs

Tableau 4 : liste des rôles utilisateurs de la sécurité

Utilisateur final	Il s'agit des personnes qui vont utiliser l'outil contenant l'information, dans lequel elle sera traitée
Business owner	Il s'agit de la ou les personne(s) qui sont responsables de l'information par rapport à sa disponibilité, sa confidentialité et son intégrité

Source : Ejzyn, A. et Van den Berghe, T. (2018). *Cybersécurité et RGPD : protégez votre PME*. Limal. p. 168-169.

- Les référents dans l'entreprise

Tableau 5 : liste des rôles référents dans l'entreprise de la sécurité

Direction	La direction décide des objectifs liés à la sécurité de l'information
Responsable de la sécurité des systèmes d'information (CISO)	Personne qui assure la mise en œuvre pratique du plan de sécurité et s'occupe de la gestion quotidienne de celle-ci
Coordinateur sécurité	Personne de référence qui assure un appui dans la mise en pratique du plan de sécurité. En fonction de la taille de l'entreprise, il peut être associé à un département, une entité, …
Responsable informatique	Personne qui va maintenir le système d'information mais également qui va aider à le développer

Source : Ejzyn, A. et Van den Berghe, T. (2018). *Cybersécurité et RGPD : protégez votre PME*. Limal. p. 168-169 ; ANSSI. (2020). *Panorama des métiers de la cybersécurité*. France : ANSSI. p. 8-33.

- Les externes à l'entreprise

Tableau 6 : liste des rôles externes à l'entreprise de la sécurité

Fournisseur(s)	Prestataire externe qui met à disposition un outil ou une infrastructure utilisée dans le projet de sécurité (expl. : application web dans le cloud)
Auditeur(s) externe(s)	Spécialistes externes à l'entreprise dont le rôle est de faire le monitoring et de certifier les systèmes d'information mis en place au sein de l'entreprise

Consultant(s)	Il peut être consultant en informatique ou en sécurité. Il va fournir des recommandations à l'entreprise dans le but de répondre aux objectifs de la politique de sécurité.

Source : Ejzyn, A. et Van den Berghe, T. (2018). *Cybersécurité et RGPD : protégez votre PME*. Limal. p. 168-169.

- Les nuisibles

Tableau 7 : liste des rôles nuisibles de la sécurité

Hacker	Personne qui tente d'accéder à un serveur pour l'endommager ou pour demander une rançon en contournant les protections mises en place
Espion	Personne qui va s'introduire dans un serveur pour y voler des informations. Cela peut être une personne interne à l'entreprise
Fraudeur	Personne qui va tenter de soutirer des informations ou des données par le biais, par exemple, d'emails de phishing
Cybercriminel	De manière plus générale, il s'agit d'une personne qui va commettre un crime via des outils informatique grâce à sa maitrise des technologies digitales

Source : Ejzyn, A. et Van den Berghe, T. (2018). *Cybersécurité et RGPD : protégez votre PME*. Limal. p. 168-169.

2. La démarche de gestion de sécurité de l'information

Tout comme pour la gestion des incidents, la démarche de gestion de sécurité de l'information est axée sur l'amélioration continue. En se basant notamment sur la roue de Deming (voir ANNEXE 2 : La roue de Deming), l'idée étant de mettre en place un processus itératif qui va permettre de définir un niveau de sécurité à atteindre et à maintenir (Ejzyn et Van den Berghe, 2018). C'est une pratique qui est également avancée par Cartau (2018).

Le but étant d'éviter d'éventuels incidents, la démarche de gestion de sécurité de l'information est généralement déployée à partir d'une gestion des risques. On part des menaces potentielles pour en déduire les risques dans le but de déterminer des mesures de sécurité adéquates à déployer. C'est une manière de faire qui est préconisée par la norme ISO 27000 (cf. infra p. 26), référentiel international en matière de sécurité de l'information. Plusieurs méthodes de gestion des risques existent. Certaines seront développées dans un prochain chapitre (cf. infra p. 27).

La gestion de la sécurité est un processus long et couteux, l'axer sur une démarche d'amélioration continue permettra cependant d'améliorer le processus et d'en augmenter le niveau de sécurité. C'est en améliorant de manière continue la démarche mise en place que l'entreprise va développer une maturité avancée face à la sécurité de l'information.

Dans ce chapitre seront développées les raisons pour lesquelles la gestion de la sécurité de l'information est importante pour les organisations. Il sera ensuite proposé une démarche de gestion de la sécurité de l'information, basée sur les bonnes pratiques de la norme ISO 27001. On fera également un point sur la gestion du changement, étape indispensable dans la mise en place d'un projet.

2.1. La gestion de la sécurité de l'information

Nous l'avons vu avec les enjeux (cf. supra p. 10), la sécurité de l'information s'étend au-delà du système d'information. C'est pourquoi la gestion de la sécurité de l'information doit être réalisée en profondeur, pour éviter qu'un élément impliqué dans le système d'information soit oublié. La gestion de la sécurité s'étend sur trois niveaux (Ejzyn et Van den Berghe, 2018), impliquant à chaque fois différents acteurs devant collaborer ensemble :

- Le niveau stratégique : il concerne la direction de l'entreprise qui va être amené à déterminer les différents objectifs qui doivent être atteints grâce à la mise en place d'une gestion de la sécurité de l'information. Cela implique la définition d'une stratégie et d'une politique de sécurité.
- Le niveau tactique : il permet de définir un plan de sécurité, en fonction de la nature du projet. Cela va impliquer différents acteurs ayant toujours le même rôle. Un plan de sécurité permet d'établir une liste d'actions précises à effectuer en vue d'atteindre les objectifs fixés en matière de sécurité. Une équipe doit être formée, dans laquelle on retrouvera à minima un ou plusieurs chefs de projet, un responsable informatique ainsi qu'un responsable de la sécurité.
- Le niveau opérationnel : il consiste en l'implémentation des actions établies dans le plan de sécurité. Cela concerne l'entièreté des acteurs du projet, et requière une sensibilisation de ceux-ci face à la gestion de sécurité mise en place.

2.2. Les étapes d'une gestion de la sécurité de l'information

Comme expliqué, la démarche de gestion de la sécurité de l'information est un processus impliquant plusieurs niveaux managériaux de l'entreprise. En se référant à la roue de Deming, le processus de démarche de gestion de la sécurité se déroule en quatre phases : planifier, réaliser, vérifier et agir (PDCA). Chaque phase du projet de gestion de sécurité de l'information est structurée en différentes étapes cruciales (voir ANNEXE 3 : Structure d'un projet de sécurité), notamment développées sur base de la démarche proposée par Ejzyn et Van den Berghe (2018), qui se sont eux-mêmes basés sur la norme ISO 27000. Ces différentes étapes seront détaillées dans les prochains sous-chapitres.

2.2.1. Définir une stratégie de sécurité

La stratégie de sécurité de l'information permet de déterminer le périmètre de la sécurité ainsi que les domaines à sécuriser. Cette stratégie va définir les démarches du projet de sécurité de l'entreprise pour qu'il y ait une harmonie générale. En rédigeant une stratégie de sécurité, l'entreprise va se positionner en matière de sécurité et s'engager à en respecter les termes. Dans certains cas, la stratégie de sécurité peut servir de base pour préciser des objectifs à atteindre ainsi que leurs indicateurs de mesures.

En plus d'établir le périmètre de la sécurité, la stratégie de sécurité précise les différentes responsabilités des acteurs concernés par l'implémentation et le contrôle de celle-ci. C'est à eux par exemple que revient le choix de déléguer certains aspects de la sécurité de l'information à des partenaires certifiés. C'est également dans le cadre de cette stratégie

qu'une entreprise va se positionner quant au choix de se référer à un référentiel métier spécifique.

La stratégie de sécurité n'est pas essentielle, si elle a été intégrée directement dans la politique de sécurité. On dit d'ailleurs qu'elle sert souvent d'intermédiaire dans la définition d'une politique de sécurité (Ejzyn et Van den Berghe, 2018). Sa mise en place dépend de la taille et de la structure organisationnelle de l'entreprise.

2.2.2. Définir une politique de sécurité

La politique de sécurité détermine les processus à mettre en place pour appliquer la stratégie de sécurité dans le but de maximiser la sécurité informatique de l'organisation. Il s'agit tout d'abord de déterminer les objectifs de cette politique et de décider des principaux besoins de l'entreprise en termes de sécurité.

C'est également dans la politique de sécurité que l'entreprise va déterminer tous les risques potentiels ainsi que la manière dont ils vont être pris en compte pour définir les meilleures mesures à adopter dans la mise en place d'une gestion de sécurité appropriée. Cela s'élabore en deux étapes (Une politique de sécurité de l'information, 2021) :

1. Établir la liste des actifs de l'entreprise ainsi que les menaces qui pèsent sur elle ;
2. Élaborer des mesures adéquates pour faire face aux risques encourus par l'entreprise en fonction des menaces identifiées.

La politique de sécurité doit être un document compréhensible et accessible par l'ensemble des acteurs et des salariés car elle représente les lignes directrices à suivre en termes de sécurité de l'information.

2.2.3. Gestion des risques

La gestion des risques est « la discipline qui s'attache à identifier, évaluer et prioriser les risques relatifs aux activités d'une organisation suivant une approche méthodique afin de réduire et contrôler la probabilité des événements redoutés, et réduire l'impact éventuel de ces évènements » (Saraydaryan J., s.d., p. 10). Elle permet donc d'anticiper et de mieux appréhender un projet et de ne pas être pris au dépourvu si un évènement inattendu se réalise. Comme précité (cf. supra p. 18), la démarche de gestion de sécurité de l'information d'une entreprise est généralement déployée à partir d'une élaboration des risques qu'elle encoure. Ces risques sont identifiés lors de l'élaboration de la politique de sécurité.

Nous avons pu constater dans les chapitres précédents que de nombreux risques peuvent survenir en matière de sécurité de l'information. Il est important de distinguer les risques informatiques et les risques métiers pour que le système d'information soit le mieux sécurisé.

L'évaluation des risques permettra de déterminer l'ordre de priorité de traitement de ceux-ci mais aussi la manière dont on va les traiter. Il existe plusieurs méthodes d'évaluation et de traitement des risques, certaines seront abordées dans un prochain chapitre (cf. infra p. 27).

a. *Évaluation des risques*

Il est malheureusement impossible de traiter l'ensemble des risques qui pèsent sur une entreprise, c'est pourquoi il faut déterminer les plus critiques d'entre eux afin de les limiter au maximum. L'évaluation des risques se déroule selon un cycle de quatre étapes. On parle de cycle car les risques doivent être réévalués régulièrement du fait de leur évolution constante.

Tableau 8 : Les quatre étapes d'évaluation du risque

Établir le contexte	Il s'agit de délimiter la gestion des risques, notamment en établissant les échelles d'évaluation de risques ainsi que le niveau acceptable des risques par l'entreprise.
Identifier les actifs	Il faut que l'entreprise identifie les actifs de support (matériel, logiciel, locaux, …) et les actifs essentiels (données clients, processus de traitement, …) qui doivent être protégés face aux incidents de sécurité de l'information. Il est important de répertorier ces différents actifs et de les trier en fonction de leurs besoins en sécurité, et cela en fonction des principes fondamentaux de la sécurité de l'information (cf. supra p. 5).
Identifier les risques potentiels	Il s'agit d'identifier les menaces potentielles qui pourraient nuire à la sécurité mais il est également important d'identifier les différentes vulnérabilités des actifs de support car nous le savons, ce sont les vulnérabilités qui créent les menaces et la combinaison des deux qui crée le risque (cf. supra p. 6).
Analyser les risques	L'analyse de risques résulte d'un calcul de criticité des risques identifiés. La criticité est le résultat de la combinaison de l'impact qu'un risque va avoir sur l'entreprise et la probabilité d'occurrence du risque. Ces critères sont déterminés lors de l'étape d'identification du contexte de la gestion des risques. Le résultat de cette analyse figure dans un tableau et permettra de mettre en place les mesures appropriées dans le traitement des risques.

Source : Ejzyn, A. et Van den Berghe, T. (2018). *Cybersécurité et RGPD : protégez votre PME*. Limal. p. 123-132.

Les trois premières étapes de ce cycle sont généralement effectuées lors de la définition de la politique de sécurité d'une organisation. Elles servent de base à l'organisation tout entière et donc établissent l'ensemble des risques communs à chaque département de celle-ci. Dans le cas où un département doit gérer un projet de sécurité de l'information, il peut rencontrer des risques qui ne sont pas communs à l'entièreté de l'organisation et doit donc adapter la politique sécurité en rédigeant une sous-politique adaptée à ses besoins et mettre en place une gestion des risques adéquate.

Il faut cependant garder à l'esprit que la mise en place d'un système d'information peut représenter un investissement ainsi qu'une innovation pour l'organisation, et cela représente un risque réel. Dans ce cas-là il est important de faire la balance entre les menaces que cette prise de risque va impliquer et les bénéfices que cela va apporter. On parle alors de « Risk appetite ».

b. *Traitement des risques*

Le niveau de criticité d'un risque va déterminer l'approche que l'entreprise doit avoir face à ces risques. C'est lors de l'étape d'identification du contexte que le seuil de criticité accepté sera déterminé. En fonction de ce seuil, un risque sera prioritairement ou non traité. De manière générale, quatre approches sont possibles face à un risque, parmi lesquelles il est indiqué de choisir en fonction de sa criticité :

- L'acceptation du risque ; implique d'accepter le risque et d'en assumer les conséquences s'il survient. A ne pas confondre avec le « risk appetite », ici on parle des risques tolérés par l'organisation.
- L'évitement du risque ; implique de changer les processus qui peuvent faire survenir le risque en question.
- Le transfert du risque ; implique de transmettre la responsabilité de la gestion du risque à un tiers.
- La réduction du risque ; implique de réduire le niveau de criticité du risque.

Dans le cas où il faut réduire un risque, des mesures et procédures doivent être mises en place, elles sont prédéfinies dans le plan de sécurité.

2.2.4. Définir un plan de sécurité

Lorsque les mesures et procédures sont déterminées, il faut choisir celles à mettre en place en priorité. Il s'agit de déterminer la faisabilité de chaque mesure, son coût et son efficacité face au niveau de réduction du risque attendu. En fonction de leur nombre, l'organisation n'aura pas la capacité de toutes les mettre en place, il faut donc déterminer leur ordre de priorité en fonction du score de criticité obtenu lors de la réalisation de l'analyse de risques.

Le plan de sécurité est donc la liste des actions à entreprendre pour assurer la sécurité et atteindre les objectifs fixés par la politique de sécurité. Il peut être présenté par risques ou par mesures, dans tous les cas, l'idée est de pouvoir visualiser les différentes actions à entreprendre, les détails liés à leur réalisation – ressources, échéances – ainsi que les acteurs concernés par la mise en place de ces actions. Pour plus de clarté et si les mesures sont nombreuses, elles peuvent également être regroupées par thématiques.

2.2.5. Partie opérationnelle

Lorsque le plan de sécurité est rédigé, la phase de planification est terminée. On entre alors dans la phase de réalisation, soit la mise en œuvre des actions listées dans le plan de sécurité. C'est une phase qui s'exécute en deux temps ; il y a la mise en œuvre du plan sécurité mais en parallèle il est indispensable de sensibiliser les utilisateurs à ce que leurs actions peuvent engendrer en termes de menace de la sécurité du système d'information.

a. *Mise en œuvre du plan de sécurité*

Comme précité, cette étape représente l'implémentation des mesures et procédures choisies dans le plan de sécurité. Il s'agit de l'étape la plus conséquente en termes d'effort et qui va

apporter le plus de changement en fonction des actions réalisées. Chaque acteur va réaliser les mesures dont il est responsable et sera suivi de près par le responsable de la sécurité. Il faudra veiller à ce que les mesures soient correctement implémentées de manière à réduire efficacement les risques, à respecter les délais prévus et à utiliser les ressources allouées dans le plan de sécurité.

Cette mise en œuvre peut être gérée comme n'importe quel autre projet et ne nécessite donc pas d'investir dans des outils spécifiques, les acteurs peuvent utiliser des outils de gestion de projet déjà intégrés par l'entreprise.

b. Formation des utilisateurs

Un des grands enjeux de la sécurité de l'information est celui de l'humain (cf. supra p. 14) et dans ce cas-ci, des utilisateurs des systèmes. Nous l'avons vu, il est impératif d'impliquer proactivement les utilisateurs afin d'avoir leur adhésion totale dans ce genre de projet. C'est pourquoi, les informer et les former est une étape cruciale dans la réalisation d'un projet sécurité. Cela doit faire partie des mesures listées dans le plan de sécurité.

Il est cependant primordial de bien veiller à adapter la communication afin que les utilisateurs ne soient pas déstabilisés par l'aspect trop technique du projet. Une communication claire, ciblée et convaincante apportera une meilleure adhésion de leur part.

2.2.6. Évaluation de la sécurité

L'évaluation de la sécurité se déroule dans le cadre de la phase de vérification du processus d'amélioration continue. Il s'agit de vérifier que les actions réalisées ont répondu aux objectifs fixés par la politique de sécurité et qu'elles ont été efficaces de manière à sécuriser le système conformément à ce qui avait été décidé dans la politique de sécurité. C'est une étape importante lorsqu'on a une démarche de gestion de projet axée sur l'amélioration continue, car vérifier l'efficacité de ce qui a été mis en place va permettre à l'organisation de comprendre ce qui a fonctionné et d'améliorer les processus qui ont été moins efficaces.

L'évaluation de la sécurité est réalisée par le biais d'un système d'audit des systèmes d'information mis en place par l'entreprise. L'audit permet de :

- Mesurer le niveau de sécurité atteint suite à la mise en place du plan de sécurité ;
- Proposer des recommandations si une mesure mise en place n'a pas été efficace dans le but de pouvoir augmenter le niveau de sécurité ;
- Dans le cas où l'organisation est certifiée à une norme, l'audit permet de vérifier si les mesures mises en place sont conformes aux exigences de la norme.

Un audit est souvent organisé en suivant des procédures bien établies qui se déroulent en trois temps. Elles sont détaillées dans le tableau ci-dessous.

Tableau 9 : Les procédures d'audit

Avant l'audit	Le responsable de sécurité va préparer un rapport qui servira d'inventaire dans lequel on pourra retrouver le processus, les mesures et procédures choisis par l'organisation ainsi que leur mise en œuvre.
	L'auditeur sélectionné va étudier le rapport afin de préparer son audit. Dans le cas où il manque des informations dans le rapport, il doit le faire savoir au responsable de sécurité, cela figurera parmi les résultats d'audit en tant qu'amélioration à apporter.
Pendant l'audit	L'auditeur va examiner le site de l'organisation et le système d'information mis en place. Il agrémentera, le cas échéant, le rapport de ses observations. Dans certains cas, un auditeur peut s'aider d'une checklist contenant les exigences à respecter imposées par une norme.
Après l'audit	L'auditeur va rédiger un rapport d'audit dans lequel il fera part de ses observations à l'intention de la direction de l'organisation.

Source : Ejzyn, A. et Van den Berghe, T. (2018). *Cybersécurité et RGPD : protégez votre PME*. Limal. p. 138.

Il est recommandé que l'auditeur ne soit pas un acteur impliqué dans la gestion de sécurité de l'information et que le système d'audit soit techniquement distinct du système de gestion de la qualité. Cependant, le système d'audit contiendra des informations qui peuvent s'avérer sensibles, il sera donc indispensable de le sécuriser également.

2.2.7. Maintenance de la sécurité

La maintenance de la sécurité est la dernière étape de la gestion du projet et représente la phase d'action dans la roue de Deming. Le processus itératif qu'implique la roue de Deming rend la démarche de gestion de sécurité de l'information permanente. Cela implique une adaptation continue des procédures et mesures adoptées notamment car elles permettent de détecter de nouvelles vulnérabilités qui devront être sécurisées, mais elles peuvent également identifier de nouveaux risques.

L'itération du cycle va impacter le système mis en place qui va constamment évoluer. Cette évolution impliquera une mise à jour des procédures et des mesures adoptées. Il en va de même dans le cas où l'organisation fait évoluer son activité et donc son système d'information. Cette évolution d'activité peut nécessiter une mise à jour des besoins en sécurité et donc impliquer une adaptation des procédures et mesures. Toutes ces évolutions permettent à l'organisation d'augmenter le niveau de maturité de son système de sécurité.

Malgré la réduction des risques par les mesures et procédures implémentées, il est rarement possible de réduire un risque à 100%, surtout que la technologie est en constante évolution. Dans le cas où le risque n'a pas bien été réduit, il faudra relancer le processus de gestion de projet.

2.3. La gestion du changement

Les mesures choisies et implémentées vont avoir un impact sur l'ancien système, modifiant ainsi la manière de l'utiliser mais également de se comporter. En plus d'apporter du changement sur le système en lui-même, elles vont apporter du changement auprès des

utilisateurs et donc sur leurs habitudes et leurs mentalités, ce qui risque de bousculer leur équilibre.

La gestion du changement est cruciale dans la démarche d'un nouveau projet, quel que soit son but, car c'est ce qui va permettre d'accompagner les utilisateurs dans l'acceptation et l'adoption de ce changement. L'impact que ce changement va avoir sur les utilisateurs est inévitable, il faut donc le gérer à la source et jusqu'à ce qu'il soit accepté, au point de faire partie de la culture de l'entreprise. Il s'agit d'un point si important, qu'il peut devenir un risque à part entière s'il n'est pas géré convenablement. La gestion du changement doit commencer dès le lancement d'un projet et se gérer en parallèle à ce projet.

Il existe dans la littérature, plusieurs modèles qui permettent de structurer sa gestion du changement. Dans ce travail, je vais présenter le modèle de gestion du changement développé par Lewin (voir ANNEXE 4 : Le modèle de changement de Lewin). Lewin propose un modèle de changement qui se décline en trois phases (ManagerGO!, 2021, *Managez le changement en 3 étapes selon le modèle de Lewin*) :

1. La décristallisation : le but est de déclencher un sentiment d'urgence concernant le besoin de changement auprès des utilisateurs. Il faut leur apporter des preuves tangibles afin de leur prouver qu'il est temps d'apporter du changement à la situation. C'est durant cette phase que les résistances au changement vont émerger. C'est une phase qui va remettre en question les comportements et habitudes de l'organisation.
   La communication est indispensable lors de cette phase, il faut convaincre les utilisateurs que le changement est indispensable et positif pour l'organisation. Elle doit mener à l'adhésion des utilisateurs.
2. La transition : c'est durant la phase de transition que l'objectif final est défini. Il est intéressant de définir cet objectif en collaboration avec les utilisateurs, car les impliquer et les responsabiliser dès le début du processus de changement facilitera leur adhésion à la nouveauté apportée par le changement et permettra de contrôler les enjeux humains (cf. supra p. 14) que la sécurité du système d'information peut subir.
   Il faut également traiter les résistances au changement détectées lors de la précédente phase. Communiquer les bénéfices du changement et découper l'objectif final en plusieurs objectifs peut faciliter cette adhésion au changement. Chaque petite victoire est à valoriser.
3. La recristallisation : le but de cette phase est d'ancrer les nouvelles habitudes dans les processus de l'entreprise. La communication est tout aussi importante que lors de la phase précédente car même si de nouvelles habitudes ont été créées, il faut que perdure la mobilisation des utilisateurs.

La gestion du changement est un processus long mais indispensable. Il permettra d'accompagner au mieux les utilisateurs d'un nouveau système d'information et de les conscientiser sur les risques de sécurité qu'encoure l'entreprise dans le cas où ils ne changent pas leurs habitudes.

3. Normes de sécurité et méthodes d'analyse de risques

Ce chapitre est structuré en lien avec la norme internationale ISO 27000, référentiel en matière de sécurité de l'information. Comme précité, cette norme conseille de gérer la sécurité de son système d'information à partir d'une gestion des risques. Dans ce chapitre, je présenterai donc la famille ISO 27000 ainsi qu'une liste non exhaustive des différentes méthodes d'analyse de risques qui existent.

3.1. La famille ISO 27000

L'organisation internationale de normalisation (ISO) n'est inconnue pour personne. Ce groupe d'experts international est à l'origine de nombreuses normes de management, servant de référence en termes de bonnes pratiques dans de multiples domaines.

Parmi ces normes, il existe la famille de norme ISO 27000 qui est constituée d'un ensemble de normes dans le domaine de la sécurité de l'information dont le but est de standardiser et faciliter sa gestion. Sa démarche est calquée sur la norme ISO9000, probablement la norme la plus connue internationalement, soit axée sur l'amélioration continue. Elle est constituée de nombreuses normes mais ce chapitre ne présentera que les plus pertinentes. Il s'agit d'une vue d'ensemble de ce que cela représente, ainsi que les différents termes et définitions liées à ce domaine. Il s'agit d'une norme qui peut être appliquée à tout type d'organisation. La norme définit la sécurité de l'information comme étant la « *protection de la confidentialité, de l'intégrité et de la disponibilité de l'information* » (Organisation internationale de normalisation, s.d., point 3.28).

Tableau 10 : Liste non-exhaustive de normes de la famille ISO 27000

ISO/IEC 27001:2013	Norme qui présente les exigences à respecter pour mettre en place un système de management de sécurité de l'information. Elle est la plus connue de la famille ISO27000 et s'adapte à tout type d'organisation.
ISO/IEC 27002:2013	Norme qui présente les bonnes pratiques en matière de système de management de sécurité de l'information. Elle est le complément de la norme ISO 27001.
ISO/IEC 27003:2017	Norme qui propose les lignes directrices à suivre pour mettre en place un système de management de sécurité de l'information.
ISO/IEC 27004:2016	Norme qui propose les lignes directrices à suivre pour mesurer la sécurité d'un système de management de sécurité de l'information. Elle est en lien avec les exigences avancées par la norme ISO 27001.
ISO/IEC 27005:2018	Norme qui propose les lignes directrices à suivre pour mettre en place un système de management de sécurité de l'information par une approche de gestion des risques.
ISO/IEC 27007:2020	Norme qui propose les lignes directrices à suivre pour mettre en place un système de management des audits adapté au système de management de sécurité de l'information.

Source : ISO (s.d.), *L'exploration spatiale à son apogée.* Récupéré le 3 mai 2021 de https://www.iso.org/fr/home.html.

Bien qu'on parle de certification, une organisation peut simplement s'inspirer de ces normes afin de faciliter la mise en place d'un système de management de sécurité de l'information structuré. En effet, le processus de certification est long et couteux, ce qui n'est pas à la portée de tous. Cependant, dans certains cas précis, les parties prenantes à une entreprise peuvent fortement recommander à celle-ci de se certifier, car cela implique une rigueur des processus dans la continuité.

3.2. Les méthodes d'analyse de risques de sécurité de l'information

La famille de normes ISO27000 propose une méthodologie de mise en place d'un système de gestion de sécurité de l'information en adoptant une approche de gestion des risques, sans pour autant proposer une méthode d'analyse de risques spécifiques. C'est à l'organisation de choisir la méthode qui lui convient le mieux. Il existe de nombreuses méthodes d'analyse de risques, je vais en présenter trois.

Tableau 11 : liste des différentes méthodes d'analyse de risques de sécurité de l'information

EBIOS	La méthode EBIOS a été élaborée par l'ANSSI (ANSSI, 2018), ce qui fait de cette méthode une référence en matière d'analyse de risques numériques. Elle s'applique à toute organisation, indépendamment de sa taille et de son secteur d'activités. Elle peut être implémentée dès la mise en place d'un système d'information mais également à un système d'information existant. C'est une méthode qui est itérative, sous le principe du PDCA. Elle propose une méthodologie en cinq ateliers (voir ANNEXE 5 : La méthode EBIOS) : • Cadrage et socle de sécurité • Sources de risque • Scénarios stratégiques • Scénarios opérationnels • Traitement du risque Elle a une approche top-down. C'est une méthode claire et exhaustive mais qui est lourde à mettre en place. Elle propose peu d'outils fonctionnels
MONARC	La méthode MONARC a été développée par le service luxembourgeois de sensibilisation et de prévention sur la sécurité de l'information (CASES, 2021) et est déclinée de la norme ISO27005. Il s'agit d'une méthode itérative qui se décline sur base des critères de sécurité choisis par l'organisation. Elle propose une méthodologie en quatre phases : • Établissement du contexte • Modélisation du contexte • Évaluation et traitement des risques • Implémentation et monitoring Cette méthode s'applique à toute organisation et a pour avantage de proposer des risques récurrents dans les différentes entreprises ayant déjà adopté cette méthode.
MEHARI	La méthode MEHARI a été développée par le CLUSIF et permet de gérer le système de sécurité de l'information et d'évaluer les risques. Elle est conforme à la norme ISO27005, elle est donc facilement applicable dans une démarche de gestion de la sécurité de l'information basée sur la norme ISO27001. Elle propose une méthodologie en trois phases (BPMS, s.d.) : • La phase préparatoire

	• La phase d'analyse des risques • La phase de planification du traitement des risques

L'utilisation d'une méthode d'analyse de risques permet d'avoir une approche globale et complète, rapide et efficace. Elle va impliquer toute la chaine de décision et va apporter une uniformité au projet.

Partie 2 : Mise en œuvre

La revue de la littérature en première partie a permis de poser un cadre sur ce que représente la sécurité de l'information ainsi que de mettre en avant une démarche recommandée à adopter pour mener à bien un projet de gestion de la sécurité de l'information. Je vais à présent vous expliquer comment j'ai mis en pratique cette connaissance dans le cadre de ma mission au sein de l'entreprise Solvay et plus précisément au département analyse de Bruxelles, afin de proposer une solution adéquate. Mais pour ce faire, il est important avant tout que vous compreniez bien le contexte dans lequel l'organisation évolue et la situation actuelle à laquelle elle est confrontée.

L'arrivée de la nouvelle CEO en 2018 Ilham Kadri (cf. supra p. 1) a amené son lot de changements, notamment avec l'élaboration de la nouvelle stratégie du groupe. Cette stratégie nommée G.R.O.W. (voir ANNEXE 6 : La stratégie G.R.O.W.) a pour but de transformer les processus mis en place au sein du groupe afin de les simplifier. Ce qui permet au groupe Solvay d'évoluer au niveau de son organisation et de sa culture, et ainsi de s'adapter à ses clients et à son environnement qui évolue sans cesse et rapidement.

Parmi les objectifs que vise cette nouvelle stratégie, la digitalisation occupe une place importante. Le but est d'accélérer la croissance du groupe en améliorant les effectifs opérationnels notamment grâce à la digitalisation, afin de les simplifier. La stratégie G.R.O.W. apporte également une nouvelle vision au groupe, qui a la volonté de s'unifier et de garantir une meilleure collaboration homogénéisée entre les différents sites, afin de former une « Team Solvay ».

Cet objectif de digitalisation impacte directement la sécurité de l'information, puisqu'il va engendrer une réorganisation de l'information chez Solvay, notamment par l'implémentation de nouveaux outils de gestion qui permettront d'alléger et de simplifier certains processus. C'est le cas notamment pour les centres de Recherche et Innovation (R&I) qui ont la volonté de mettre en place un outil collaboratif de gestion de laboratoire. C'est dans ce contexte que la réalisation de ce travail m'a été demandée.

Dans cette partie, il y aura une brève explication de l'organisation de l'entreprise, car cela a un impact sur les différents projets digitaux du groupe. Ensuite, un chapitre sera dédié à la sécurité de l'information déjà en place au sein de Solvay. Je présenterai également le projet de mise en place d'un outil de gestion de laboratoire dans son ensemble, en expliquant l'organisation du projet et les personnes concernées. Enfin, il y aura un focus sur le département analyse, qui est à l'origine de ce travail, ainsi qu'une description de l'outil dont il est question. Ces informations me permettront ensuite de proposer une solution en vue de la mise en place d'un outil collaboratif de gestion de laboratoire. Des interviews avec des experts et des acteurs du projet ont été réalisées pour alimenter cette partie (voir ANNEXE 7 : Tableau des interviews).

4. L'organisation de Solvay

Pour bien fonctionner, une entreprise d'une telle ampleur se doit d'adopter une gouvernance d'entreprise bien organisée afin de garantir sa pérennité. Le groupe Solvay s'organise autour de quatre composantes :

- La direction générale, composée du conseil d'administration et du comité d'exécution, dont l'objectif est d'assurer la pérennité de l'entreprise, de développer son capital humain et d'accroitre sa valeur (Rapport Annuel Intégré, 2018).
- Les Global Business Units (GBU) sont les moteurs de la croissance de Solvay. Elles sont regroupées au sein de segments opérationnels et opèrent mondialement, au plus proche des clients et des marchés. Elles jouissent d'une large autonomie, et peuvent être considérées comme de petites entreprises indépendantes qui peuvent développer leurs activités et les conduire à leur manière.
- Les directions fonctionnelles – plus communément appelées fonctions – sont acteurs dans plusieurs GBU et peuvent leur servir de support. Parmi ces directions fonctionnelles, on retrouve notamment la fonction « Recherche & Innovation » (R&I). Il s'agit de la fonction concernée par la question de recherche.
- Le Solvay Business Services (SBS) qui est en charge de la gestion opérationnelle des finances, des ressources humaines, des achats et de l'IT.

Lorsqu'une fonction ou une GBU désire lancer un projet, quel que soit son objectif, le processus se fait en collaboration avec SBS. L'organisation d'une telle collaboration sera détaillée dans le cadre de l'explication du projet de mise en place de l'outil collaboratif dont il est question dans ce travail (cf. infra p. 31).

5. La sécurité de l'information chez Solvay

Solvay est une entreprise dans le secteur de la chimie orientée vers l'innovation et la durabilité. Le groupe est spécialisé dans les matériaux avancés et la chimie de spécialité. Ces pratiques donnent lieu à de nombreuses recherches scientifiques ce qui représente l'avantage concurrentiel du groupe. Les connaissances, les recherches et les chercheurs de Solvay sont les éléments qui font de Solvay le leader sur le marché de la chimie.

La digitalisation des processus et des ressources de l'entreprise impose la mise en place d'une gestion de la sécurité de l'information de pointe, ce qui n'a pas été le cas durant de nombreuses années. Dans ce chapitre, on abordera la manière dont Solvay organise la sécurité de l'information ainsi que les différents acteurs impliqués dans cette organisation.

5.1. L'organisation de la sécurité chez Solvay

La taille de l'entreprise impose une gouvernance de gestion de la sécurité pour éviter le chaos. SBS est l'organisation qui décide et gère tout ce qui peut toucher à la digitalisation. En effet, certifié ISO27001, SBS dispose des outils nécessaires pour mettre en place une gestion de la sécurité de l'information. Cependant, l'aspect sécurité a longtemps été négligé et limité

uniquement à la gestion de la confidentialité des données. Or, pour garantir une bonne sécurité de l'information, les principes d'intégrité et de disponibilité sont également à prendre en compte.

Comme précité, l'arrivée de la nouvelle CEO a amené son lot de changements, notamment en matière de sécurité de l'information. Suite à une analyse de risques réalisée pour l'ensemble du groupe Solvay, il s'est avéré que le risque le plus élevé auquel il fait face est celui de la sécurité. La démarche d'analyse de risque adoptée par le groupe tient compte des menaces et des risques. Des actions sont mises en place au niveau du groupe afin de protéger ses différents sites, mais aussi les informations et les personnes. La démarche de sécurité de l'information se fait par une approche de gestion des risques pilotée par trois organes de gouvernance (Rapport annuel Solvay, 2020) :

- Un conseil de sécurité, qui s'occupe de l'aspect stratégique de la gestion des risques ;
- Un « Security Leadership Committee » qui supervise les activités liées à la sécurité ;
- Un groupe de travail de Coordination de la sécurité, qui fait fonctionner le programme de sécurité du groupe.

Un programme de cybersécurité a été mis en place en 2020 et est gouverné par les trois organes précités.

La crise sanitaire a imposé la montée du télétravail, ce qui a exposé le groupe à de nouvelles menaces. Ceci a accéléré le besoin de réorganisation de la sécurité et de la révision de ce qui était en place jusqu'à présent. C'est en avril 2021 que la politique de sécurité a été révisée et remise à jour pour prendre en compte le groupe dans son ensemble. Elle a été rédigée de manière à correspondre à l'ensemble des organisations qui forment le groupe Solvay en tenant compte des grands risques qu'il encourt. Cette politique de sécurité sert de base mais doit être adaptée et complétée par toute fonction ou GBU qui se lance dans un projet de sécurité.

5.2. Le groupe sécurité chez Solvay

Pour répondre aux exigences d'un grand groupe tel que Solvay, le groupe sécurité est hiérarchisé afin de couvrir au mieux l'ensemble des fonctions et des GBU. Voici comment sont hiérarchisés les différents rôles au sein du groupe sécurité de Solvay :

Tableau 12 : Les rôles de la sécurité chez Solvay

Rôle	Description de la fonction
Comité d'exécution	Décider des objectifs de la sécurité de l'information pour le groupe Informer annuellement le Conseil d'Administration de la sécurité de l'information
Directeur de la sécurité (CSO)	Coordonner toutes les activités relatives à la sécurité au niveau mondial
Chief information security officer (CISO)	Coordonner toutes les activités liées à la sécurité. Il dépend du directeur de la sécurité de l'information

Security Champion	Sert de correspondant auprès d'une fonction ou d'une GBU pour s'assurer que la politique de sécurité est prise en charge

6. La mise en place d'un outil de gestion de laboratoire au sein de Solvay

La demande de mise en place d'un outil collaboratif de gestion de laboratoire a été introduite par la fonction R&I, pour l'ensemble des huit laboratoires d'analyse que compte le groupe Solvay. Il s'agit d'un gros projet, qui impacte de nombreuses personnes et qui doit répondre à plusieurs exigences en fonction des besoins des laboratoires d'analyse.

Dans ce chapitre, nous verrons premièrement ce qu'est un outil de gestion de laboratoire, en quoi il consiste et pourquoi il est important dans un département analyse. Ensuite, nous détaillerons l'organisation de ce projet.

6.1. Qu'est-ce qu'un outil de gestion de laboratoire ?

Un outil de gestion de laboratoire (LIMS) permet de gérer les principaux processus d'un laboratoire grâce à un outil centralisé. Un processus de laboratoire part d'une demande d'analyse d'un client jusqu'à l'obtention des résultats en suivant tout son cheminement, c'est-à-dire la gestion de la demande, la réception des échantillons, les équipements et méthodes à utiliser pour réaliser l'analyse, ainsi que la rédaction et l'envoi des résultats.

Un outil tel que le LIMS est important pour un département analyse, parce qu'un département analyse fonctionne par prestation, et traite un grand nombre de demandes d'analyse. Gérer cela sans utiliser un outil adéquat rend souvent difficile la mise en place d'une traçabilité efficace. Cet outil permet également de mettre en place une planification du travail, de mieux gérer le temps et donc d'accroitre l'efficacité.

6.2. L'organisation du projet LIMS

Le projet LIMS a débuté en 2019, suite à la demande de la fonction R&I qui était désireuse d'acquérir un outil LIMS collaboratif. Jusqu'à présent, chaque département analyse possédait son propre LIMS, provenant de fournisseurs différents, rendant compliquée la collaboration entre les départements. Cette collaboration est pourtant primordiale car elle permet de mieux gérer les différentes demandes d'analyse, et ce pour plusieurs raisons :

- Si un laboratoire est surchargé, il peut déléguer certaines demandes à d'autres laboratoires ayant la même expertise ;
- Si un laboratoire possède un équipement qui est en maintenance et qui est requis pour une analyse, il peut déléguer cette demande à un laboratoire qui possède le même équipement.

Les besoins de la fonction ont été recueillis par les managers des différents laboratoires concernés en relation avec la personne référente de R&I et ont été transmis à SBS afin de les

transformer en projet (voir figure 2). SBS a ensuite contacté des fournisseurs de LIMS, afin de leur soumettre ce qu'on appelle un « Request for Information » (RFI). Les fournisseurs vont ensuite envoyer un dossier à Solvay dans lequel ils vont répondre au RFI. C'est un groupe projet Solvay, composé de personnes de chez SBS mais également de la R&I, qui va analyser ces rapports et faire une pré-sélection. Les fournisseurs sélectionnés seront ensuite invités à réaliser une démonstration de leur outil en présence du groupe Solvay, qui va sur cette base finaliser son choix.

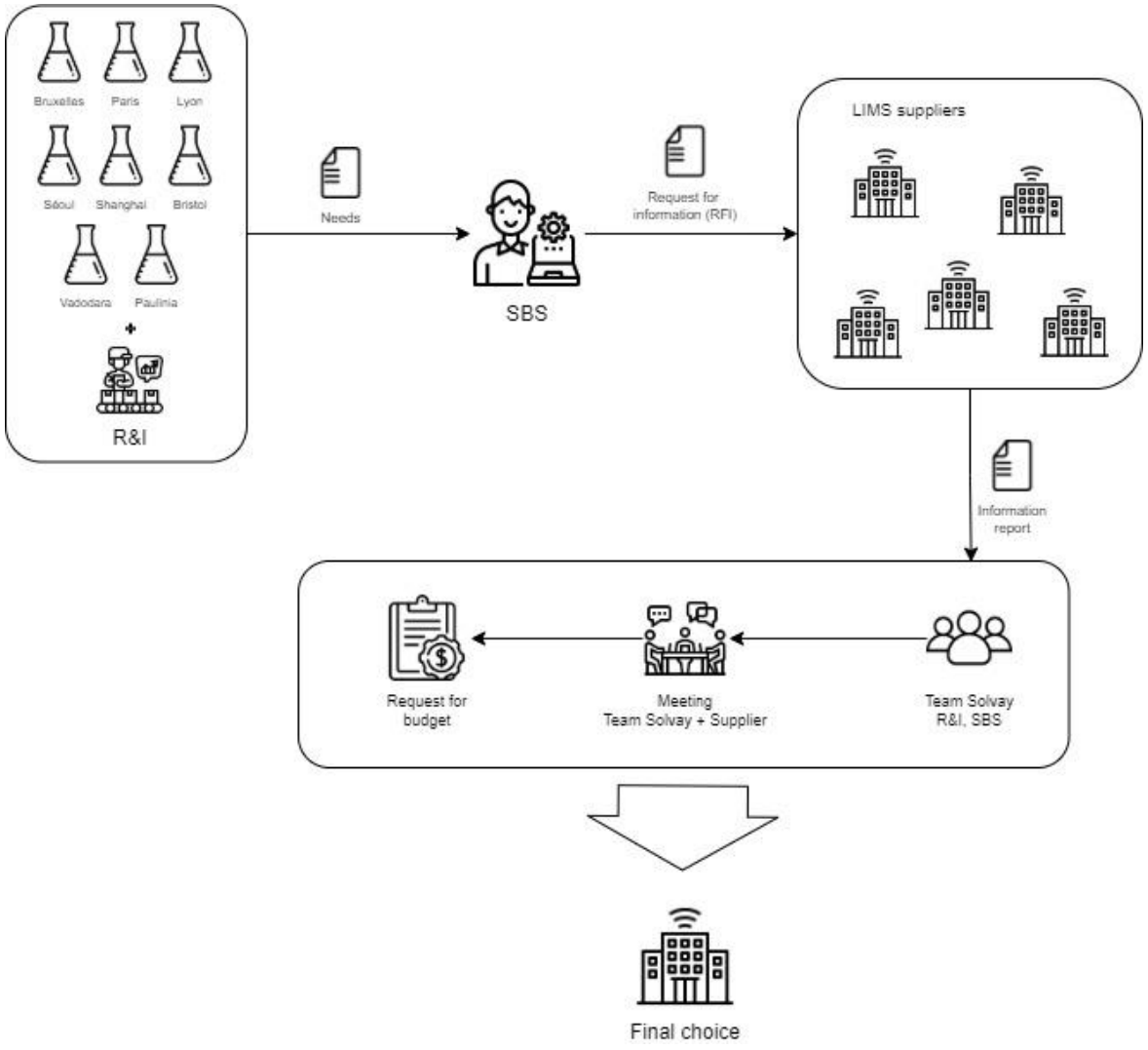

Figure 2 : Organisation du projet LIMS
Source des images : https://www.flaticon.com/

Deux chefs de projet ont été désignés (un chef de projet SBS et un chef de projet R&I), dont le rôle a été de déterminer les risques métiers et techniques engendrés par le projet LIMS en collaboration avec les différents managers des laboratoires concernés (qui ont chacun apporté leur liste de risques métiers). Les risques techniques sont déterminés par le chef de projet SBS. Il est à noter que la fonction SBS couvre un grand nombre de risques, notamment les risques que le groupe Solvay dans son ensemble peut encourir (soit liés au réseau, à l'infrastructure, à la gestion des accès, ...) et qui s'appliquent de facto à un projet.

Solvay n'impose pas de méthode particulière d'analyses de risques, mais propose néanmoins des templates. Une dizaine de risques indépendants aux laboratoires a été définie selon quatre thématiques :

- Risques liés à la relation avec le fournisseur ;
- Risques liés aux évènements externes (tel que la crise sanitaire) ;
- Risques liés aux équipes Solvay (ils doivent en effet compter sur la disponibilité des équipes Solvay qui mettront en place les infrastructures qu'impose le projet) ;
- Risques liés aux futurs utilisateurs de l'outil.

Ils ont également établi un plan de « change management » destiné à l'ensemble des futurs utilisateurs du LIMS. Le projet ayant démarré en 2019, il n'a pas été réalisé en relation avec la politique de sécurité de l'information validée en avril 2021.

7. La mise en place de l'outil dans le département analyse

Les précédents chapitres ont permis une visualisation d'ensemble du projet LIMS. Cependant, et nous l'avons évoqué, chaque entité doit déterminer ses propres limites en fonction de l'usage qu'elle va faire de l'outil afin de dresser une liste de risques métiers. Ce qui nous amène à l'essentiel de ce travail : en effet, ce travail concerne l'entité R&I de Bruxelles, et plus précisément le département analyse, ainsi que ses laboratoires, pour lequel je travaille en tant que stagiaire depuis deux ans.

Dans ce chapitre, je vous présenterai le département analyse et son organisation. Ensuite je vous présenterai l'outil LIMS, ses caractéristiques, son fonctionnement et son organisation par rapport à l'utilisation du département. Ce chapitre permet d'approfondir le cadre de ce travail pour nous emmener vers la solution recommandée.

7.1. Le département analyse de Bruxelles

Le département analyse est géré par Véronique Mathieu et compte 38 collaborateurs. Sa mission est de réaliser des analyses chimiques et des tests de matériaux pour ses clients (Département Analyse Solvay, Politique qualité [Intranet], 2019). Les analyses sont réalisées dans quatre laboratoires : les laboratoires de chimie organique et de chimie inorganique, faisant tous deux partie du pôle d'activité des analyses chimiques, et les laboratoires de testing et de physico-chimie et microscopie, qui font partie du pôle d'activité de caractérisation des matériaux.

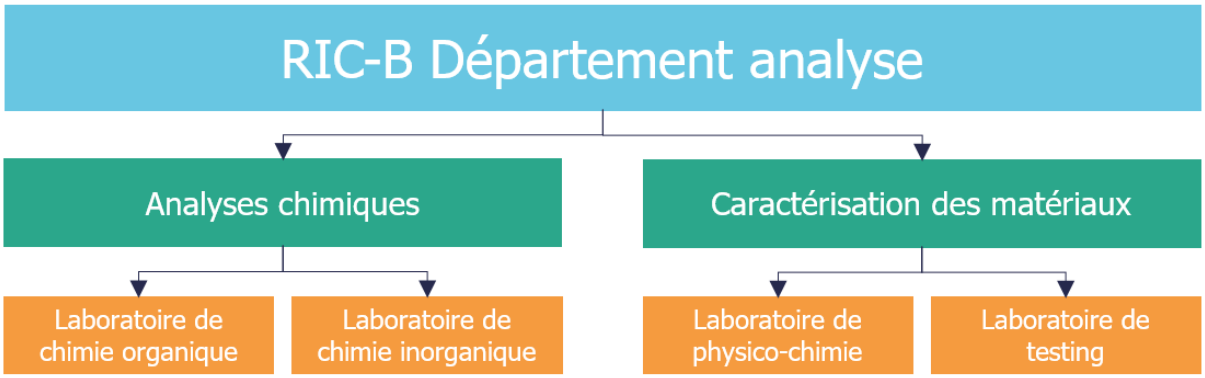

Figure 3 : Organisation des laboratoires du département analyse Bruxelles

Le département a pour mission (Département Analyse Solvay, Manuel Qualité [Intranet], 2020) d'assurer des prestations pour les entités internes, soit les différentes GBU ou fonctions, ainsi que pour des clients externes à l'entreprise. Afin de garantir l'excellence opérationnelle, le département travaille en étroite collaboration avec les autres centres de recherches répartis à travers le monde, ainsi qu'avec les universités et les centres de recherches reconnus.

7.2. La présentation de l'outil

L'outil sélectionné par le groupe Solvay est un LIMS qui se présente sous application web. Le choix de l'application web répond au désir des différents laboratoires concernés d'avoir un outil moderne, flexible et collaboratif. L'enjeu de cet outil est de respecter les aspects confidentiels des données tout en permettant une collaboration et un partage de certaines informations entre départements.

Ci-dessous, les caractéristiques de l'outil ainsi que son fonctionnement sont présentés, afin de bien délimiter le contexte du projet lié à la question de recherche.

7.2.1. Les caractéristiques de l'outil choisi

L'outil possède trois caractéristiques recherchées par les départements analyse :

- La modernité : cet outil collaboratif sera facile d'accès avec une interface propre ;
- La flexibilité : dans sa mise en place mais également dans sa réception de demandes clients, qui doit être possible pour des clients internes mais également externes à l'entreprise, et avec des niveaux de confidentialité différents, qui seront détaillés dans le prochain paragraphe (cf. infra p. 35) ;
- La facilité : l'outil va permettre une meilleure gestion des demandes clients et donc faciliter l'organisation du travail des analystes.

Le LIMS sélectionné est une application web de la solution cloud d'Amazon Services (AWS) de type IaaS (cf. supra p. 12). Ce type de cloud a été sélectionné pour répondre à l'exigence des normes d'export control auxquelles Solvay est soumise. Le département analyse de Bruxelles n'est pas concerné par cette norme. Prendre un LIMS de type IaaS permet aussi à Solvay de garder la main sur tout ce qui concerne les accès, les serveurs, les clés d'inscription et les données.

L'outil est une solution centralisée, il s'agit d'un serveur de base de données Solvay qui contiendra l'ensemble des données des sites concernés par l'outil. Cependant, il y a une ségrégation des données ; en fonction du rôle de l'utilisateur qui se connecte, l'outil détermine les données auxquelles il peut avoir accès. Les différents rôles sont présentés dans le prochain paragraphe.

7.2.2. Le fonctionnement de l'outil

L'outil permet de regrouper l'ensemble des processus impliqués dans la demande d'analyse d'un client. Il permet également de lier les différentes bases de données utilisées dans ces processus. Cet outil va en outre permettre de planifier le travail des analystes, d'analyser ce qui entre et ce qui sort, de gérer au jour le jour le travail à effectuer et d'anticiper les besoins. Ceci facilitera la gestion de la traçabilité d'une demande (on pourra en effet facilement associer l'objet de la demande, qui fait la demande, qui va la gérer, où sont les échantillons à analyser, à qui faut-il envoyer les résultats de l'analyse, …).

Prendre connaissance du fonctionnement de l'outil en fonction de l'utilisation que va en faire le département, permet de déceler certains points sensibles qui peuvent générer des vulnérabilités. En effet, le département analyse de Bruxelles travaille avec des clients externes, ce qui n'est pas le cas des autres départements, il est donc exposé à différentes menaces qui doivent être prises en compte. Avoir une vision schématisée du processus du département est donc important, le voici (voir ANNEXE 8 : Flux d'activité d'une demande d'analyse) :

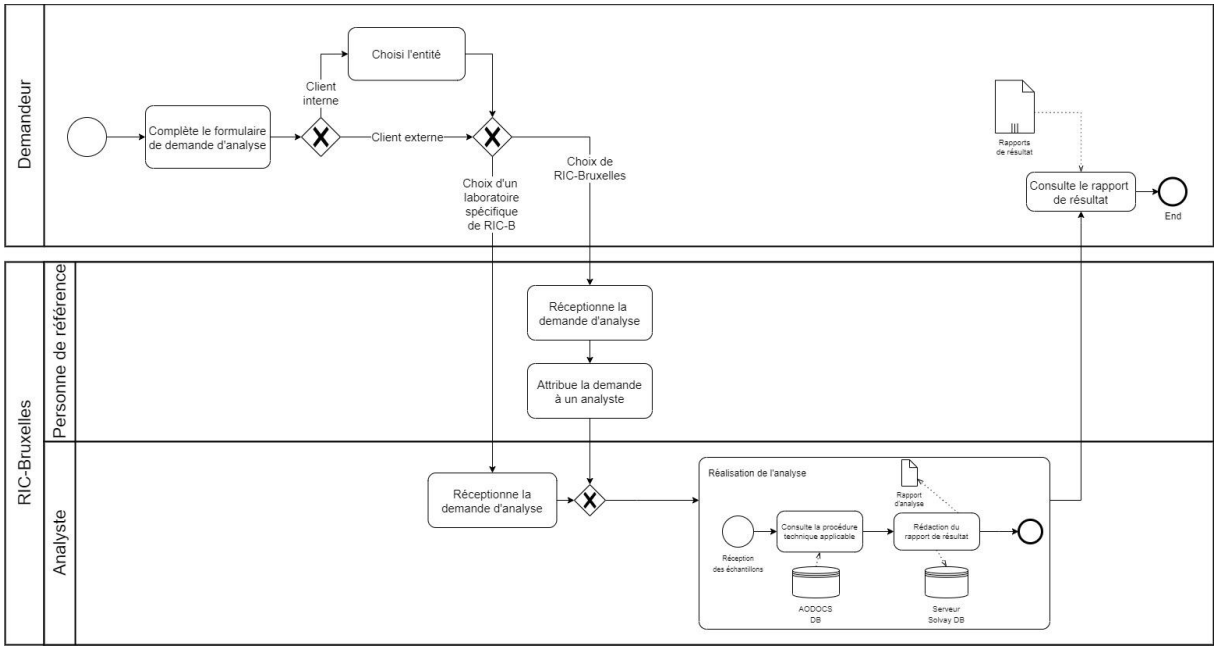

Figure 4 : Flux d'activité d'une demande d'analyse
Schéma réalisé sur https://app.diagrams.net/

Si la demande d'analyse est réalisée par un client interne à l'entreprise, celui-ci a le choix parmi les entités du groupe pour faire exécuter le travail. S'il s'agit d'un client externe, il n'aura accès qu'aux entités avec qui il a un contrat. Les demandes d'analyse de clients externes ne seront visibles que par les analystes de l'entité concernée. Dans les deux cas, une demande peut être faite directement à un laboratoire défini – dans tel cas les analystes de ce laboratoire choisiront

la personne qui réalisera le travail –, ou à une entité – c'est alors une personne de référence de l'entité qui assignera la demande à une technique spécifique et à un analyste de laboratoire.

Le LIMS permet aussi d'accéder aux autres outils utilisés par les entités. Par exemple, pour le département analyse, l'outil LIMS permettra notamment d'accéder à ses différentes bases de données AODOCS ainsi qu'au Shared Drive Google du département. Ces accès sont possibles via des liens URL, en conséquence on ne peut pas afficher un document d'un outil externe directement dans le LIMS. Cependant, ces interactions ne font pas partie du contexte de ce travail, les risques liés ne seront donc pas traités ici.

Lorsque le rapport de résultat est finalisé, il est stocké dans un serveur base de données de Solvay. Le client demandeur a accès à un dossier comprenant l'ensemble de ses rapports de résultats, et il peut les consulter depuis son interface dans le LIMS.

a. L'organisation de l'outil

Étant donné que l'outil peut être utilisé par différents laboratoires, il est organisé en fonction des différentes entités concernées. On retrouve trois niveaux : la fonction R&I, les différentes entités R&I et les laboratoires de chaque entité.

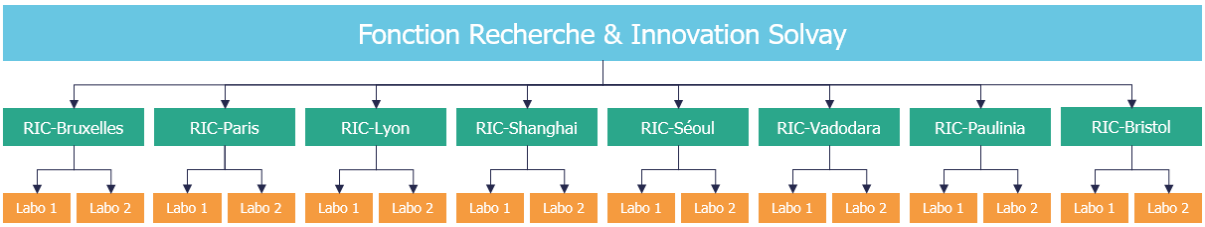

Figure 5 : Organisation des laboratoires de la fonction R&I

Chaque demande d'analyse est associée à un laboratoire d'une entité (RIC). Les accès aux demandes sont gérés par entité.

Une demande d'analyse peut être introduite selon trois niveaux, à déterminer par le demandeur lorsqu'il effectue sa demande :

- Non-confidentiel : la demande est visible pour toutes les entités Solvay
- Confidentiel : la demande est visible uniquement pour l'entité concernée
- Confidentiel export control : la demande est visible uniquement pour les analystes accrédités export control de l'entité concernée

b. La gestion des accès de l'outil

La sécurité de l'outil est garantie par la gestion des accès de celui-ci. Les accès se font en fonction de rôles définis dans l'application et qui sont liés aux utilisateurs. On retrouve quatre types de rôles, présentés dans le tableau ci-dessous :

Tableau 13 : Les rôles des utilisateurs du LIMS

Analyste	Il a accès aux données liées aux demandes des clients de l'organisation à laquelle il est attaché. Seul un analyste accrédité aux normes d'export control pourra accéder aux demandes de ce type.
Administrateur local	Il gère les utilisateurs et a accès aux droits spécifiques de son organisation.
Administrateur global	Il gère les demandes d'amélioration du système avec le fournisseur. Il a accès aux données des administrateurs locaux et des analystes.
Demandeur	Il a accès au formulaire de demande d'analyse et à la liste de ses propres demandes déjà effectuées ainsi qu'à un dossier depuis lequel il peut consulter ses rapports de résultats.

Étant une application web, l'outil LIMS sera accessible grâce à un lien URL. En fonction de son rôle, l'utilisateur devra s'identifier :

- Demandeurs : chaque demandeur se verra attribuer un identifiant et un mot de passe, lui permettant d'accéder à l'outil LIMS. Pour recevoir ces accès, il devra figurer sur la liste des demandeurs gérée par l'administrateur local.
- Analystes et administrateurs : ces utilisateurs sont internes à Solvay et leur accès est soumis à la méthode de gestion des accès choisie par le groupe, qui est le SSO. Son authentification se fait automatiquement depuis son matériel Solvay lorsqu'il est sur le réseau Solvay.
  Depuis un autre réseau, l'utilisateur devra passer par le VPN de Solvay pour accéder à l'outil.

8. La solution proposée pour le projet

Maintenant que le contexte dans lequel évolue le département analyse et sa situation ont été expliqués, je peux m'atteler à la mise en pratique des connaissances acquises depuis le début de ce travail. La mission qui m'a été confiée est celle d'épauler Véronique Mathieu dans la mise en place de la gestion de sécurité de l'information lors de l'implémentation de l'outil LIMS au sein de son département.

J'ai décidé d'appliquer la démarche de gestion de sécurité de l'information présentée lors de la première partie de ce travail. Tout d'abord parce que d'un point de vue méthodologique, c'est la démarche à suivre pour mener à bien un tel projet, mais aussi parce que cela va apporter une approche holistique du projet au département analyse.

Dans ce chapitre, j'aborderai la politique de sécurité que Solvay a validée en avril 2021, car elle détermine les domaines à sécuriser ainsi que les processus à mettre en place dans le but de maximiser la sécurité de l'information du groupe. Elle présente aussi les principaux besoins de l'entreprise en termes de sécurité. En accord avec cette politique, je proposerai une méthode d'analyse de risques simple et complète qui permettra ensuite de passer à la proposition de recommandations pour le département.

8.1. L'application de la politique de sécurité du groupe Solvay

Comme expliqué, la politique de sécurité a été revue et validée en avril 2021. Elle n'a donc pas pu être prise en considération lors de l'analyse de risques réalisée par les chefs de projet qui a précédé la mise en place du LIMS. Il est cependant important de la prendre en compte afin de s'assurer que les risques identifiés par le groupe Solvay ont été considérés.

Parmi l'ensemble des risques détectés par le groupe sécurité Solvay pour l'ensemble de l'entreprise, cinq sont à prendre en compte dans le contexte du projet LIMS :

Tableau 14 : Risques principaux du groupe Solvay

P.CS.CR.01	Vol de propriété intellectuelle
P.CS.CR.02*	Fuite de données contrôlées conduisant au non-respect de la réglementation américaine et européenne en matière d'exportation
P.CS.CR.05	Failles de données du fournisseur tiers
P.CS.CR.10	Fuite de données non intentionnelle par des utilisateurs légitimes
P.CS.CR.11	Fuite de données intentionnelle par des utilisateurs légitimes

Source : Solvay. (2021). *Information and Cyber Security Policy* [Intranet]. Bruxelles : Solvay.

*Il est à noter que le risque P.CS.CR.02 concerne la norme d'export control qui ne concerne pas le département analyse. Cependant, il est tout de même important que le département soit au courant de l'ensemble des risques, car si un incident survient, cela peut avoir des conséquences sur l'ensemble de l'outil.

La politique de sécurité a été définie par le groupe sécurité de Solvay, et concerne l'ensemble des sites et entités du groupe. Cependant, elle est non-exhaustive et doit être adaptée aux besoins et exigences de chaque entité. Il est impératif qu'elle soit prise en compte lors de la mise en place d'un projet, mais une sous-politique peut être réalisée pour et en fonction de chaque projet.

8.1.1. Les actifs du département

Dans un groupe tel que Solvay, il est normal de rédiger des sous-politiques. En effet, le groupe est responsable des risques qui concernent l'entièreté du groupe. Chaque GBU, fonction, entité ou département, en fonction de ses besoins, peut, en s'inspirant et en prenant en compte la politique globale du groupe, rédiger sa sous-politique. La sous-politique de sécurité a la même fonction que la politique de sécurité : elle sert à établir la liste des actifs et des menaces liées qui pèsent sur l'organisation. Grâce à cela, on pourra par la suite établir une liste plus exhaustive des risques.

En accord avec la manager du département analyse Véronique Mathieu, j'ai dressé la liste des actifs concernés par le projet LIMS, que j'ai séparé par type : actifs essentiels et actifs de support :

Tableau 15 : Liste des actifs essentiels et de support du département analyse pour le projet LIMS

Actifs essentiels	Actifs de support
Demandes clients	LIMS
Résultats d'analyse	
Liste des clients internes	
Liste des clients externes	
Procédures techniques	Base de données AODOCS*

*A rappeler que les bases de données externes au LIMS ne font pas partie du contexte, elles ne représentent donc pas un actif pris en compte dans cette analyse de risques. Cependant, les procédures techniques seront accessibles par un lien URL depuis le LIMS, ces dernières sont donc prises en compte dans cette analyse de risques.

8.1.2. Les risques du département analyse

L'analyse de risques qui suit concerne spécifiquement le département analyse de Bruxelles dans le cadre de l'implémentation du LIMS et de son utilisation, je ne prendrai donc pas en compte les risques généraux déjà couverts par le groupe Solvay qui concernent principalement les risques environnementaux, réseaux et infrastructures. Les risques liés à la relation avec le fournisseur étant pris en charge par l'analyse de risques du projet global, ils ne seront pas pris en compte non plus. C'est pourquoi j'invite le département à se référer aux nouvelles sous-politiques de sécurité publiées par le groupe sécurité de Solvay pour tout ce qui sort du périmètre de la présente analyse.

La liste de risques que j'ai rédigée pour le département analyse de Bruxelles a été validée par Véronique Mathieu. Il s'agit de risques qui peuvent avoir un impact opérationnel sur le département :

Tableau 16 : Liste de risques pour le département analyse de Bruxelles

Actions non autorisées	Utilisation non autorisée de l'outil
	Corruption des données
	Traitement illégal de données
Pannes techniques	Panne de l'outil
	Dysfonctionnement de l'outil
Nuire à l'information	Vol de documents
	Détérioration de l'outil
	Divulgation de l'information
	Espionnage à distance
Nuire aux fonctions	Erreur d'utilisation
	Abus de droits
	Détérioration des droits

Source : ISO. (2008). *ISO/IEC 27005:2008 Annex C & D.* ISO/IEC 2008.

8.2. La réalisation d'une analyse de risques

Pour rappel, les menaces vont exploiter les vulnérabilités que les actifs de support présentent, ce qui risque de les affecter et donc d'avoir un impact sur le système d'information lui-même. Implémenter une gestion d'analyse de risque est donc fortement recommandé, surtout en matière de sécurité de l'information. Elle se fait dans un cycle d'amélioration continue, soit le PDCA, ce qui implique une révision constante des risques et des mesures mises en place pour les diminuer.

Des méthodes d'analyse de risques ont été présentées dans un précédent chapitre (cf. supra p. 27), cependant, j'ai utilisé une méthode d'analyse simplifiée qui me permettra de fixer plus facilement les priorités au niveau du traitement des risques. Cette méthode a été élaborée par Alain Huet, ancien CISO du Fedict (SPF Technologie de l'information et de la communication), elle est donc légitime (Sécurité de l'information et gestion du risque, 2019). J'ai volontairement choisi, sous les conseils de mon promoteur, de ne pas utiliser une des méthodes présentées précédemment car elles sont lourdes à mettre en place et impliquent le recours à des experts en sécurité. De plus, Solvay n'impose pas de méthode spécifique d'analyse de risques.

Cette méthode se décline en trois étapes, et prend en compte les différentes étapes à suivre d'une démarche de gestion des risques, en alignement avec ce que la norme ISO27005 suggère, comme on peut le constater dans le tableau ci-dessous :

Tableau 17 : Comparaison de la méthode Fedict et de la démarche de gestion des risques ISO27005

Méthode du Fedict	Démarche ISO27005
Etablissement du contexte	Etablissement du contexte
Appréciation des risques	Identification des risques
	Analyse des risques
	Évaluation des risques
Plan de traitement	Traitement des risques
	Acceptation des risques

L'avantage de l'utilisation de cette méthode simplifiée est que cela permettra au département analyse de l'alimenter par la suite sans avoir besoin de recourir aux services d'un expert en sécurité. C'est une méthode efficace, simple et rapide à mettre en place. L'objectif de cette méthode est que le business owner soit l'acteur principal de la gestion de risque (Sécurité de l'information et gestion du risque, 2019).

8.2.1. L'établissement du contexte

Le contexte a déjà partiellement été établi : cette analyse de risque concerne le département analyse de Bruxelles. Il s'agit également de l'étape durant laquelle on détermine les critères de base d'évaluation des risques. Dans cette méthode, deux métriques sont à déterminer : la métrique d'impacts et la métrique de défauts de sécurité.

a. *Métrique d'impacts*

La métrique d'impacts consiste à définir la nature des conséquences des menaces sur le département ainsi que les critères d'acceptation selon un niveau de gravité allant de 1 à 4. Ils ont été déterminés en collaboration avec Véronique Mathieu.

Gravité	Nature des conséquences				
	Pertes financières (milliers €) **F**	Compétitivité **C**	Secret **S**	Réputation **R**	Divulgation d'informations classifiées **D**
1	1 - 10	Réorganisation des activités de gestion	-	Rédiger un rapport de résultats erronés non transmis au client	Diffusion restreinte (autres entités)
2	10 – 100	Perte de clients internes et/ou externes (< 2)	*Divulgation de données commerciale*	*Transmettre un rapport avec des résultats erronés au client*	Confidentiel (par rapport à l'entité)
3	100 – 500	Perte de clients internes et/ou externes (> 2)	Divulgation de résultats d'analyse	Transmettre un rapport de résultats erronés sans qu'il soit utilisé par le client	Secret (par rapport au monde extérieur)
4	> 500	Arrêt des activités du département	Divulgation de procédures techniques	Transmettre un rapport de résultats erronés utilisés par le client	Très secret (par rapport aux internes)

Les lettres F, C, S, R et D serviront lors de l'étape qui consiste à déterminer, pour chaque actif, l'impact sur le département (cf. infra p. 42).

N.B. : Commentaires par rapport à certains critères (en *italique* dans le tableau) :

- Divulgation de données commerciales : il s'agit de données propres concernant les différents clients du département
- Transmettre un rapport au client avec des résultats erronés : il diffère du critère suivant car dans ce cas-ci, un analyste se rend compte de l'erreur, dans l'autre cas, c'est le client qui s'en rend compte.

b. *Métrique de défauts de sécurité*

Nous l'avons vu, plusieurs principes fondamentaux doivent être pris en compte pour garantir la sécurité d'un système. La métrique de défauts de sécurité permet d'établir la liste des défauts que chaque principe pourrait avoir.

Disponibilité	Indisponibilité du système : 5 minutes 1 heure 1 jour 1 semaine < 1 semaine
Intégrité	Altération (si on s'en rend compte à temps) Destruction (si on ne s'en rend pas compte)
Confidentialité	Divulgation d'informations
Preuve	Enregistrements non probants
Légalité	Transgression (accord de confidentialité, publication externe dans approbation du service juridique)

8.2.2. L'appréciation des risques

Dans cette méthode, l'étape d'appréciation des risques englobe l'identification, l'analyse et l'établissement des risques. C'est une étape qui se fait en trois temps :

a. Pour chaque actif, déterminer l'impact sur le département ;
b. Pour chaque risque, déterminer l'évènement redouté en fonction de l'origine de la menace et de la vulnérabilité du système ;
c. Pour chaque actif, déterminer l'impact que les différents évènements peuvent avoir.

C'est grâce à cette dernière étape qu'on pourra élaborer des mesures de sécurité et donc rédiger un plan de traitement des risques.

a. L'impact sur le département pour chaque actif

Afin de déterminer pour chaque actif l'impact qu'un défaut de sécurité peut avoir sur le département, la méthode propose de suivre un template : pour chaque actif, on réalise un tableau dans lequel on indique la ou les conséquence(s) que peut engendrer chaque défaut ainsi que le niveau maximum de gravité acceptable.

Expl. : Si le LIMS est indisponible pendant 24 heures, quelles sont les conséquences de cette indisponibilité et quel est le niveau de gravité de cette conséquence.

Actif : Demandes clients		Conséquences F	C	S	R	D	Maximum
Disponibilité	Indisponibilité : 5 minutes						
	1 heure						
	1 jour	1					1
	1 semaine	3	2				3
	> 1 semaine	4	3				4
Intégrité	Altération (on s'en rend compte à temps)	1		2	3	1	3
	Destruction (on ne s'en rend pas compte)	3	1	3	4	4	4
Confidentialité	Divulgation d'informations	2	2	2		4	4
Preuve	Enregistrements non probants	2	2	3	4	4	4
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	3	3	2		4	4

Actif : Résultats d'analyse		Conséquences F	C	S	R	D	Maximum
Disponibilité	Indisponibilité : 5 minutes						
	1 heure						
	1 jour		2		2		2
	1 semaine	2	3	3	4	3	4
	> 1 semaine	3	3	3	4	3	4
Intégrité	Altération (on s'en rend compte à temps)	2	1	3	3		3
	Destruction (on ne s'en rend pas compte)	3	3	3	4		4
Confidentialité	Divulgation d'informations	2	3	3		4	4
Preuve	Enregistrements non probants	3	3		4		4
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	4	3	3		3	3

Actif : Liste des clients internes		Conséquences F	C	S	R	D	Maximum
Disponibilité	Indisponibilité : 5 minutes						
	1 heure						
	1 jour						
	1 semaine	1	1				1
	> 1 semaine	1	2				2
Intégrité	Altération (on s'en rend compte à temps)	1	1	2			2
	Destruction (on ne s'en rend pas compte)	2	3	3			3
Confidentialité	Divulgation d'informations	2	3	2		3	3
Preuve	Enregistrements non probants		1	3			3
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	2	3	2		3	3

		Conséquences					
Actif : Liste des clients externes		F	C	S	R	D	Maximum
Disponibilité	Indisponibilité : 5 minutes						
	1 heure						
	1 jour						
	1 semaine	1	1				1
	> 1 semaine	1	2				2
Intégrité	Altération (on s'en rend compte à temps)	1	1	2			2
	Destruction (on ne s'en rend pas compte)	2	3	3			3
Confidentialité	Divulgation d'informations	2	3	2		4	4
Preuve	Enregistrements non probants		1	3			3
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	3	3	2		3	3

		Conséquences					
Actif : Procédures techniques		F	C	S	R	D	Maximum
Disponibilité	Indisponibilité : 5 minutes						
	1 heure						
	1 jour						
	1 semaine	2	1		1		2
	> 1 semaine	3	2		2		3
Intégrité	Altération (on s'en rend compte à temps)	1	1		2		2
	Destruction (on ne s'en rend pas compte)	4	3		4		4
Confidentialité	Divulgation d'informations	4	4	4		3	4
Preuve	Enregistrements non probants	3	3		4		4
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	4	4	4		3	4

		Conséquences					
Actif : LIMS		F	C	S	R	D	Maximum
Disponibilité	Indisponibilité : 5 minutes						
	1 heure						
	1 jour						
	1 semaine	2	2				2
	> 1 semaine	3	3				3
Intégrité	Altération (on s'en rend compte à temps)	2	2				2
	Destruction (on ne s'en rend pas compte)	3	4				4
Confidentialité	Divulgation d'informations	3	3	3		4	4
Preuve	Enregistrements non probants	3	3		4		4
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	3	3	3		4	4

b. *Liste des évènements redoutés en fonction des menaces*

Lorsqu'une menace exploite une vulnérabilité, alors un évènement redouté peut survenir, c'est pour cela qu'une gestion des risques est importante. En fonction des risques qui ont été listés précédemment (cf. supra p. 39), on va déterminer son origine et son type de vulnérabilité, ce qui nous permettra d'avoir une liste d'évènements redoutés.

Il y a plusieurs origines possibles à une menace, nous nous concentrerons sur les suivantes :

- Technique
- Erreur humaine
- Action délibérée

Nous ne prenons pas en compte les menaces d'origine naturelle car elles sont déjà gérées par l'analyse de risques globale du projet LIMS.

Il existe plusieurs types de vulnérabilité qui peuvent survenir en fonction de l'évènement. J'avais précédemment expliqué que les risques liés aux infrastructures et aux réseaux n'étaient pas pris en compte dans cette analyse, cependant, certains risques peuvent quand même faire survenir des vulnérabilités sur ceux-ci, c'est pourquoi ils sont repris dans les différents types de vulnérabilité.

Evènement redouté : Utilisation non autorisée de l'outil		ER 1
Origine de la menace	Technique	
	Erreur humaine	x
	Action délibérée	x
Vulnérabilité	Matériel	
	Logiciel	x
	Réseau	x
	Personnel	x
	Organisation	x

Evènement redouté : Corruption des données		ER 2
Origine de la menace	Technique	
	Erreur humaine	x
	Action délibérée	x
Vulnérabilité	Matériel	
	Logiciel	x
	Réseau	
	Personnel	
	Organisation	x

Evènement redouté : Traitement illégal de données		ER 3
Origine de la menace	Technique	
	Erreur humaine	x
	Action délibérée	x
Vulnérabilité	Matériel	
	Logiciel	x
	Réseau	
	Personnel	x
	Organisation	x

Evènement redouté : Panne de l'outil		ER 4
Origine de la menace	Technique	x
	Erreur humaine	
	Action délibérée	
Vulnérabilité	Matériel	x
	Logiciel	
	Réseau	
	Personnel	
	Organisation	x

Evènement redouté : Dysfonctionnement de l'outil		ER 5
Origine de la menace	Technique	x
	Erreur humaine	
	Action délibérée	
Vulnérabilité	Matériel	
	Logiciel	x
	Réseau	
	Personnel	
	Organisation	

Evènement redouté : Vol de documents		ER 6
Origine de la menace	Technique	
	Erreur humaine	x
	Action délibérée	x
Vulnérabilité	Matériel	x
	Logiciel	x
	Réseau	
	Personnel	x
	Organisation	x

Evènement redouté : Détérioration de l'outil		ER 7
Origine de la menace	Technique	
	Erreur humaine	
	Action délibérée	x
Vulnérabilité	Matériel	
	Logiciel	x
	Réseau	
	Personnel	
	Organisation	

Evènement redouté : Divulgation de l'information		ER 8
Origine de la menace	Technique	
	Erreur humaine	x
	Action délibérée	x
Vulnérabilité	Matériel	
	Logiciel	
	Réseau	
	Personnel	
	Organisation	

Evènement redouté : Espionnage à distance		ER 9
Origine de la menace	Technique	
	Erreur humaine	
	Action délibérée	x
Vulnérabilité	Matériel	
	Logiciel	
	Réseau	x
	Personnel	
	Organisation	

Evènement redouté : Erreur d'utilisation		ER 10
Origine de la menace	Technique	
	Erreur humaine	x
	Action délibérée	x
Vulnérabilité	Matériel	x
	Logiciel	x
	Réseau	
	Personnel	x
	Organisation	x

Evènement redouté : Abus de droits		ER 11
Origine de la menace	Technique	
	Erreur humaine	x
	Action délibérée	x
Vulnérabilité	Matériel	
	Logiciel	x
	Réseau	
	Personnel	
	Organisation	x

Evènement redouté : Falsification des droits		ER 12
Origine de la menace	Technique	
	Erreur humaine	x
	Action délibérée	x
Vulnérabilité	Matériel	
	Logiciel	x
	Réseau	x
	Personnel	
	Organisation	

c. *Impact des évènements sur les actifs*

Maintenant que nous avons déterminé l'impact des actifs sur le département et la liste des évènements redoutés en fonction de l'origine de la menace et du type de vulnérabilité, il est possible de déterminer l'impact de ces évènements sur les actifs.

Pour cela, nous allons reprendre chaque actif dans un tableau, avec pour chaque défaut de sécurité le niveau maximal de gravité que nous avons déterminé précédemment, et voir quels évènements redoutés vont avoir un impact sur ces actifs.

Actif : Demandes clients		Max	E 1	E 2	E 3	E 4	E 5	E 6	E 7	E 8	E 9	E 10	E 11	E 12
Disponibilité	Indisponibilité : 5 minutes													
	1 heure													
	1 jour	1	x			x	x	x	x		x			
	1 semaine	3	x			x	x	x	x		x			
	> 1 semaine	4	x			x	x	x	x		x			
Intégrité	Altération	3	x	x	x		x		x		x	x	x	x
	Destruction	4	x	x	x		x		x		x	x	x	x
Confidentialité	Divulgation d'informations	4	x	x	x		x		x	x	x		x	x
Preuve	Enregistrements non probants	4	x	x	x		x		x		x	x	x	x
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	4	x	x	x		x		x	x	x		x	x

Actif : Résultats d'analyse		Max	E 1	E 2	E 3	E 4	E 5	E 6	E 7	E 8	E 9	E 10	E 11	E 12
Disponibilité	Indisponibilité : 5 minutes													
	1 heure													
	1 jour	2	x	x		x	x	x	x		x	x		
	1 semaine	4	x	x		x	x	x	x		x	x		
	> 1 semaine	4	x	x		x	x	x	x		x	x		
Intégrité	Altération	3	x	x	x				x		x	x		x
	Destruction	4	x	x	x				x		x	x		x
Confidentialité	Divulgation d'informations	4	x	x	x			x	x	x	x	x	x	x
Preuve	Enregistrements non probants	4	x		x						x	x		x
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	3	x	x	x			x		x	x	x	x	x

Actif : Liste des clients internes		Max	E 1	E 2	E 3	E 4	E 5	E 6	E 7	E 8	E 9	E 10	E 11	E 12
Disponibilité	Indisponibilité : 5 minutes													
	1 heure													
	1 jour													
	1 semaine	1	x		x	x	x		x		x	x		x
	> 1 semaine	2	x		x	x	x		x		x	x		x
Intégrité	Altération	2	x	x	x		x		x		x	x	x	x
	Destruction	3	x	x	x		x		x		x	x	x	x
Confidentialité	Divulgation d'informations	3	x		x		x	x	x	x	x	x	x	x
Preuve	Enregistrements non probants	3	x	x	x		x		x		x	x	x	x
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	3	x		x		x	x	x	x	x	x	x	x

Actif : Liste des clients externes		Max	E 1	E 2	E 3	E 4	E 5	E 6	E 7	E 8	E 9	E 10	E 11	E 12
Disponibilité	Indisponibilité : 5 minutes													
	1 heure													
	1 jour													
	1 semaine	1	x		x	x	x		x		x	x		x
	> 1 semaine	2	x		x	x	x		x		x	x		x
Intégrité	Altération	2	x	x	x		x		x		x	x	x	x
	Destruction	3	x	x	x		x		x		x	x	x	x
Confidentialité	Divulgation d'informations	4	x		x		x	x	x	x	x	x	x	x
Preuve	Enregistrements non probants	3	x	x	x		x		x		x	x	x	x
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	3	x		x		x	x	x	x	x	x	x	x

Actif : Procédures techniques		Max	E 1	E 2	E 3	E 4	E 5	E 6	E 7	E 8	E 9	E 10	E 11	E 12
Disponibilité	Indisponibilité : 5 minutes													
	1 heure													
	1 jour													
	1 semaine	2									x			
	> 1 semaine	3									x			
Intégrité	Altération	2									x			
	Destruction	4									x			
Confidentialité	Divulgation d'informations	4						x		x	x		x	x
Preuve	Enregistrements non probants	4												
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	4						x		x	x		x	x

Actif : LIMS		Max	E 1	E 2	E 3	E 4	E 5	E 6	E 7	E 8	E 9	E 10	E 11	E 12
Disponibilité	Indisponibilité : 5 minutes													
	1 heure													
	1 jour													
	1 semaine	2				x	x		x			x		x
	> 1 semaine	3				x	x		x			x		x
Intégrité	Altération	2	x											x
	Destruction	4	x											x
Confidentialité	Divulgation d'informations	4	x								x		x	x
Preuve	Enregistrements non probants	4												x
Légalité	Transgression (accord de confidentialité, publication externe sans approbation du service juridique)	4	x								x		x	x

Partie 3 : Recommandations

A présent que nous avons terminé d'analyser les risques et leurs impacts sur les différents actifs du département, il est temps de les traiter. Pour rappel, le traitement des risques consiste notamment à déterminer la priorité de traitement de ceux-ci, permettant par la suite de rédiger un plan de sécurité.

Dans cette partie, je vous présente le plan de traitement des risques qui découle de l'analyse de risques, afin de savoir comment les traiter et de déterminer les mesures de sécurité à mettre en place. Ceci mènera à l'élaboration du plan de sécurité. Enfin, je proposerai un plan de gestion du changement, étape indispensable dans une gestion de projet.

9. Le plan de traitement des risques

Le plan de traitement consiste à dresser une liste de mesures qui permettront d'atténuer les risques. Elle est basée sur les risques rencontrés précédemment. Dans ce chapitre, j'ai donc élaboré une série de mesures qui visent à traiter les risques potentiels en sécurisant les différents actifs concernés, pour ensuite proposer les mesures à mettre en place, qui constitueront le plan de sécurité.

9.1. Élaboration des mesures de sécurité

Les mesures sont organisées par thèmes. Pour chaque mesure, je déterminerai un coût, l'attribut de sécurité qu'elle permet d'améliorer ainsi que l'évènement redouté qu'elle traite.

Il est à noter qu'il est recommandé d'impliquer un consultant en sécurité. Il existe chez Solvay des « security champion » pour chaque fonction ou GBU, qui ont le rôle de consultant sécurité. Pour la fonction R&I, il s'agit de Jean-Christophe Gallan, je suggère au département de s'y référer dans le futur. Je conseille au département de désigner un responsable sécurité, dont la responsabilité sera la mise en place des mesures de sécurité.

9.1.1. Mesure concernant les données

Mesure 1	Classifier les données à sécuriser

L'étape de classification des données permettra de les identifier mais également de les sécuriser. Pour chaque actif essentiel, on déterminera les données impliquées, le processus auquel il est lié ainsi que son actif de support.

Cette mesure permet de savoir quelles sont les données à protéger, et à quels niveaux elles doivent l'être.

Action	Prévention								
Coût	Initial								
Concerne	Le business owner								
Attributs améliorés	Disponibilité		Evènements traités	E1		E6		E11	x
	Intégrité			E2		E7		E12	
	Confidentialité	x		E3	x	E8	x		
	Preuve			E4		E9			
	Légalité			E5		E10	x		

Il est intéressant de mettre en œuvre cette mesure en étant accompagné du responsable de sécurité ainsi que d'un responsable informatique.

9.1.2. Mesures concernant les accès aux données

Classifier les données à sécuriser ne garantit pas à 100% leur sécurité. Je l'ai déjà mentionné lors de l'état de l'art, la gestion des accès est une des premières mesures à mettre en place dans un projet de gestion de sécurité de l'information (cf. supra p. 12).

Mesure 2	Classifier les accès autorisés

Le LIMS étant un outil qui se sécurise par la gestion des accès (cf. supra p. 36), déterminer les besoins d'accès pour chaque utilisateur est primordial. Un utilisateur ne doit pas avoir accès à des informations qui ne le concernent pas. C'est pourquoi, il est important de répertorier les différents utilisateurs et leur fonction et de tenir ces informations à jour. En effet, un utilisateur qui quitte l'organisation ne doit plus avoir accès à l'outil de même qu'un utilisateur qui change de fonction doit faire l'objet d'une adaptation de ses accès. L'élaboration d'un tableau reprenant ces données permettra une vue structurée de ce qui est mis en place au niveau des accès.

Dans le cas du LIMS, l'accès à l'outil par les utilisateurs autorisés se fait grâce à leurs identifiants généraux Solvay. Si un utilisateur change de fonction et de département, il conserve ses identifiants Solvay. Il est donc important de s'assurer qu'il n'aura plus accès à l'outil, une fois qu'il aura quitté le département. Il est à noter que, étant donné que le LIMS est utilisé par les analystes Solvay mais également par des clients externes à l'organisation, la distinction entre ces deux groupes d'utilisateurs est primordiale.

Action	Prévention								
Coût	Initial								
Concerne	L'administrateur local et le business owner								
Attributs améliorés	Disponibilité		Évènements traités	E1	x	E6	x	E11	x
	Intégrité	x		E2	x	E7		E12	x
	Confidentialité	x		E3		E8	x		
	Preuve			E4		E9			
	Légalité			E5		E10	x		

L'administrateur global du LIMS dispose d'un accès illimité à l'outil, il est donc très important de confier ce rôle à une personne de confiance.

Mesure 3	Accorder les accès strictement adaptés à la fonction de l'utilisateur

Cette mesure rejoint la précédente. Une fois les utilisateurs répertoriés selon leur fonction, il est nécessaire d'identifier les accès liés à chaque fonction. (Par exemple : un analyste n'a pas besoin d'avoir accès aux informations concernant les managers).

Comme mentionné plus haut, cette mesure doit être mise en œuvre distinctement pour les analystes, et pour les clients. Ils sont tous deux utilisateurs de l'outil, mais ne doivent pas avoir accès aux mêmes informations. (Par exemple : l'analyste n'a pas besoin d'accéder au formulaire de demande client, et le client n'a pas besoin d'accéder au processus de traitement de demande d'analyse).

Action	Prévention								
Coût	Initial								
Concerne	L'administrateur local et le business owner								
Attributs améliorés	Disponibilité	x	Évènements traités	E1	x	E6	x	E11	x
	Intégrité	x		E2	x	E7		E12	x
	Confidentialité	x		E3	x	E8	x		
	Preuve			E4		E9			
	Légalité	x		E5		E10	x		

Dans le cas du LIMS, c'est l'administrateur local qui a la main sur la gestion des accès de son entité. C'est donc important d'être vigilent quant au choix de la personne qui aura cette responsabilité.

Mesure 4	Auditer les accès aux données

Cette mesure concerne la gestion des logs abordée lors de l'état de l'art (cf. supra p. 13). Auditer les accès permet de savoir quels utilisateurs ont eu accès à quelles données. Cela pourrait paraître inutile si on met en place une classification des accès et pourtant, cela permettra d'obtenir une traçabilité précise des activités. Notamment quand le département

analyse a recours à l'expertise d'analystes externes ; ces derniers doivent pouvoir accéder aux différentes données sensibles du département, telles que les procédures techniques. Dans ce cas, il est pertinent de connaitre les données auxquelles ils ont eu accès ainsi que les actions qu'ils ont réalisées.

Le groupe Solvay a déjà été victime d'espionnage. Auditer les accès régulièrement, permet facilement de détecter un utilisateur suspect. Dans le cas où un analyste fraichement embauché décide de quitter l'entreprise, le département pourra vérifier les données auxquelles cette personne a eu accès et évaluer les risques potentiellement liés le cas échéant.

Action	Prévention								
Coût	Récurrent								
Concerne	L'administrateur local[1]								
Attributs améliorés	Disponibilité		Evènements traités	E1	x	E6	x	E11	x
	Intégrité	x		E2	x	E7	x	E12	x
	Confidentialité	x		E3	x	E8	x		
	Preuve	x		E4		E9	x		
	Légalité	x		E5		E10	x		

Le traitement des logs implique la gestion de données à caractère personnelles, le département doit donc les traiter conformément au RGPD. Le LIMS possède probablement des fonctionnalités standards de traçabilité, je conseille au département de se renseigner sur la possible exploitation de ces informations selon les règles à respecter en termes de confidentialité.

9.1.3. Mesures concernant les utilisateurs

Nous avons pu constater que la majorité des évènements redoutés ont pour origine l'erreur humaine. Des mesures concernant les utilisateurs sont donc indispensables à mettre en place. Et il est important d'impliquer proactivement les utilisateurs à cette mise en place à travers différentes actions récurrentes. Surtout lorsqu'on est dans une démarche d'amélioration continue, comme c'est le cas en gestion de projet de sécurité de l'information.

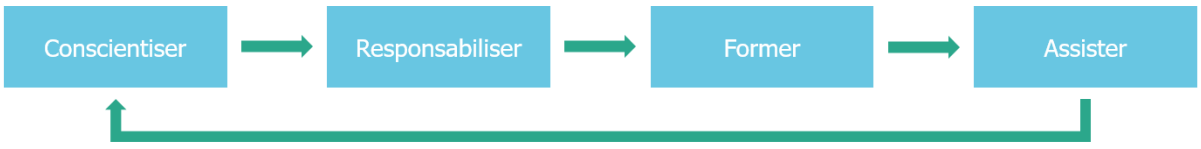

Figure 6 : Les actions à mettre en place pour impliquer les utilisateurs dans la sécurisation d'un système d'information

[1] Information à vérifier : il se pourrait que cela concerne l'administrateur global. Je n'ai pas eu la possibilité de vérifier l'information.

Source : Ejzyn, A. et Van den Berghe, T. (2018). *Cybersécurité et RGPD : protégez votre PME*. Limal. p. 46.

Les mesures développées ci-dessous, concernant les utilisateurs, suivent la figure ci-dessus :

Mesure 5	Conscientiser les utilisateurs

Dans le contexte de ce travail, les utilisateurs se divisent en deux groupes : les utilisateurs Solvay et les utilisateurs clients.

1. Les utilisateurs Solvay :

Il est important de les impliquer dès le début du projet de sécurisation de l'information, tant au niveau de son contexte, que de ses objectifs et des enjeux qu'encoure le département. Ils doivent se rendre compte des conséquences qu'un incident de sécurité peut avoir sur le département et in fine sur eux. Il est essentiel de les sensibiliser en leur exposant des exemples concrets (par exemple : si un incident survient et qu'un cybercriminel réussit à accéder aux actifs essentiels, cela peut conduire à un arrêt des activités du département, car cela va engendrer une perte de confiance des clients).

Il faut également les conscientiser sur les règles de sécurité à respecter ainsi que les actions qu'ils n'ont pas le droit de faire. Il faut leur expliquer la raison pour laquelle ils doivent suivre ces indications : donner du sens à une action la rend plus concrète et acceptable, aussi contraignante soit-elle.

Cette mesure permettra de faciliter la gestion du changement.

2. Les utilisateurs clients :

Dans le cas du LIMS, je pense qu'il est intéressant de conscientiser également les clients des différents enjeux de sécurité encourus par le département. En effet, l'utilisation qu'ils en ont peut également conduire à des incidents, même involontaires. Étant donné les relations étroites que le département entretient avec ses clients, ce sera simple à mettre en place.

Action	Prévention								
Coût	Récurrent								
Concerne	Les utilisateurs								
Attributs améliorés	Disponibilité		Évènements traités	E1		E6	x	E11	
	Intégrité	x		E2	x	E7		E12	
	Confidentialité	x		E3	x	E8	x		
	Preuve			E4		E9			
	Légalité	x		E5		E10	x		

C'est au manager, avec l'aide du responsable de sécurité, que revient cette responsabilité.

Mesure 6	Responsabiliser les utilisateurs

Une manière d'impliquer un utilisateur dans un projet est de le responsabiliser. Cela peut se faire de différentes manières :

- Lui confier des tâches à réaliser en vue de garantir la sécurité ;
- L'informer de ses propres responsabilités si un incident survient, afin de l'inciter à éviter de commettre des erreurs d'utilisation qui pourraient engendrer cet incident ;
- Lui expliquer les éventuelles sanctions qui peuvent suivre s'il a un comportement inapproprié, qui dans certains cas pourrait mener à un licenciement pour faute grave.

Le département peut élaborer une charte d'utilisation qui guidera les différents utilisateurs. Cette responsabilisation peut se faire via des newsletters, des supports visuels mais également des workshops qui permettront de les coacher.

Responsabiliser un utilisateur peut également lui permettre de déceler des comportements suspects et inappropriés et de les dénoncer.

Je conseille au département de responsabiliser ses clients par rapport aux incidents qu'ils subissent et qui peuvent in fine l'impacter (par exemple : si un client subit une attaque, cela peut avoir un impact sur l'outil LIMS et donc in fine impacter le département).

Action	Prévention								
Coût	Récurrent								
Concerne	Les utilisateurs								
Attributs améliorés	Disponibilité	x	Évènements traités	E1	x	E6	x	E11	x
	Intégrité	x		E2	x	E7	x	E12	x
	Confidentialité	x		E3	x	E8	x		
	Preuve	x		E4		E9	x		
	Légalité	x		E5		E10	x		

C'est le rôle et la responsabilité du responsable de sécurité de s'occuper de la responsabilisation des utilisateurs.

Mesure 7	Former les utilisateurs

La formation des utilisateurs à l'usage d'un nouvel outil est évidente, mais il est tout aussi important de les former aux mesures de sécurité à observer dans le cadre de cet usage.

1. Les utilisateurs Solvay

Il est indispensable que les utilisateurs soient formés à l'utilisation de l'outil, cela permet notamment d'éviter un certain nombre d'incidents commis par erreur. Mais il est également intéressant de former les utilisateurs à réagir face aux éventuelles menaces, ils pourront les

prévenir mais également réagir rapidement et efficacement, en prévenant par exemple la personne référente.

Chaque utilisateur doit bien évidemment être formé à ce qui le concerne : on ne va pas former un analyste à la gestion des accès alors que c'est de la responsabilité de l'administrateur local.

2. Les utilisateurs clients

Il est tout d'abord important que le département forme ses clients à l'utilisation du nouveau LIMS. Ensuite, il faut les former sur les éventuels incidents indirects qui peuvent impacter le département : comme expliqué ci-dessus, si un client est victime d'une attaque, celle-ci peut avoir un impact sur le LIMS, il faut que le client puisse réagir rapidement à cela en informant directement le département.

Action	Prévention								
Coût	Récurrent								
Concerne	Les utilisateurs								
Attributs améliorés	Disponibilité	x	Evènements traités	E1	x	E6		E11	x
	Intégrité	x		E2	x	E7	x	E12	x
	Confidentialité	x		E3	x	E8	x		
	Preuve	x		E4		E9			
	Légalité	x		E5	x	E10	x		

C'est le rôle du manager du département de s'assurer que les utilisateurs Solvay sont proprement formés. Cependant, la formation est réalisée par le responsable sécurité à l'échelle globale du projet. J'invite le département à se renseigner sur ce qui a été prévu à cet effet auprès des personnes référentes.

Mesure 8	Assister les utilisateurs

L'idée est de mettre en place une assistance à disposition des utilisateurs, afin de les guider s'ils sont confrontés à un incident. L'assistance peut prendre la forme d'un document reprenant les différentes actions à réaliser dans chaque cas de figure, ou d'une personne référente de support, tel qu'un référent de sécurité.

Action	Prévention								
Coût	Récurrent								
Concerne	Les utilisateurs								
Attributs améliorés	Disponibilité	x	Evènements traités	E1	x	E6	x	E11	x
	Intégrité	x		E2	x	E7	x	E12	
	Confidentialité	x		E3	x	E8	x		
	Preuve	x		E4		E9	x		
	Légalité	x		E5	x	E10	x		

9.1.4. Les mesures hors cadre

Comme déjà évoqué, certains risques ne sont pas directement liés au fonctionnement du département. Lors de l'analyse de risques, nous avons pu constater que certains évènements redoutés peuvent survenir suite à une vulnérabilité du réseau ou des infrastructures (panne, …). C'est pourquoi je propose ci-dessous des mesures liées à ces risques, le département a le choix d'en faire part aux personnes concernées. J'invite le département à se renseigner sur la prise en charge de ces mesures auprès des personnes référentes.

Mesure 9	Auditer l'utilisation du réseau

Cette mesure rejoint la mesure d'audit des accès mais à partir du réseau, qui constitue une belle porte d'entrée pour quiconque souhaite infiltrer l'outil, ou même simplement le réseau Solvay, ce qui pourrait impacter in fine le LIMS.

En auditant l'utilisation du réseau, on peut détecter si d'éventuels cybercriminels ou espions tentent d'accéder au réseau. En effet, on peut voir si plusieurs tentatives infructueuses ont été commises.

Action	Prévention								
Coût	Récurrent								
Concerne	Les chefs de projet								
Attributs améliorés	Disponibilité	x	Evènements traités	E1	x	E6	x	E11	x
	Intégrité	x		E2	x	E7	x	E12	x
	Confidentialité	x		E3	x	E8	x		
	Preuve	x		E4	x	E9	x		
	Légalité	x		E5	x	E10	x		

Cet audit peut se faire par les responsables informatiques mais également par le biais d'auditeurs externes.

Mesure 10	Protéger et contrôler strictement l'accès au cloud

Le nouveau LIMS est une application web hébergée dans le cloud (cf. supra p. 34). Ce qui expose l'outil à de nouvelles menaces, il est donc indispensable de protéger et de contrôler l'accès au cloud également.

Il est important de bien analyser les règles de responsabilité imposées par le fournisseur de cloud afin de s'assurer de bien contrôler les accès. Dans le cas du projet LIMS, cette gestion des accès est sous la responsabilité de Solvay.

Action	Prévention								
Coût	Récurrent								
Concerne	Les chefs de projet								
Attributs améliorés	Disponibilité	x	Évènements traités	E1	X	E6	x	E11	x
	Intégrité	x		E2	x	E7	x	E12	x
	Confidentialité	x		E3	x	E8	x		
	Preuve	x		E4		E9	x		
	Légalité	x		E5	x	E10	x		

9.2. Mesures de sécurité à mettre en place

Il n'est pas possible de mettre en application toutes les mesures précitées en même temps, il faut donc les prioritiser. Pour cela, j'ai procédé à leur classement selon deux axes : les évènements traités et les attributs améliorés. La mesure doit être mise en place en priorité si elle répond à ces deux critères :

- Elle permet de traiter plus de 5 évènements redoutés ;
- Elle permet d'améliorer plus de 2 attributs de sécurité.

Tableau 18 : Matrice des mesures de sécurité en fonction des évènements traités et des attributs améliorés

Mesures	Évènements traités	Attributs améliorés
Mesure 9	12	5
Mesure 10	11	5
Mesure 8	10	5
Mesure 6	10	5
Mesure 4	10	4
Mesure 7	9	5
Mesure 3	8	4
Mesure 2	7	2
Mesure 5	5	3
Mesure 1	4	1

J'invite donc le département à mettre en place dès que possible les mesures selon l'ordre de priorité défini dans le tableau ci-dessus.

9.2.1. Suggestions pour les mesures hors cadre

L'utilisation d'un VPN est déjà requise chez Solvay pour accéder à certains outils à distance. La question de recourir à l'utilisation du VPN pour accéder au LIMS pourrait être débattue étant donné que l'entreprise ne l'utilise pas pour accéder à l'entièreté de ses outils. Mais je conseille au département analyse de plaider en faveur de l'utilisation du VPN également pour accéder au LIMS à distance.

En effet, bien que l'accès à ces outils via le VPN représente une contrainte, on a pu constater que depuis que le télétravail est devenu une norme pour la majorité des entreprises, et le groupe Solvay ne fait pas exception à la règle, les cyberattaques et tentatives de phishing n'ont cessé d'augmenter (LeDevoir, 4 février 2021). Il est donc, selon moi, incontournable de sécuriser au maximum l'accès à cet outil, pour les raisons que j'ai déjà largement développées préalablement.

9.2.2. Gestion des incidents

La mise en place de mesures préventives efficaces n'empêche pas des incidents de survenir. C'est pour cela que je propose au département de suivre la démarche de gestion des incidents que j'ai présentée dans l'état de l'art (cf. supra p. 15) afin d'établir un plan de réponse aux incidents. Je propose en ce sens au département de réaliser les trois mesures suivantes :

1. Établir un plan de réponse aux incidents

   Pour cela, il est intéressant de mettre en place la première mesure que j'ai présentée, soit le fait de répertorier les différents actifs du département et de classer les données qu'ils contiennent en fonction de leurs processus.

   Pour chaque actif, il faut déterminer une liste d'actions et de procédures à mettre en place afin de traiter efficacement et entièrement un incident.

   Il est également important de tenir un registre des différents acteurs qui sont concernés ainsi que leurs contacts. Cela permettra à celui qui détecte l'incident de savoir quelle personne avertir en fonction de la nature de l'incident.

   Le plan de réponse aux incidents est un document qui doit être accessible et compréhensible par tous les acteurs concernés.

2. Détecter les incidents de sécurité

   Impliquer les utilisateurs comme je l'ai précédemment suggéré est un facteur clé dans la détection des incidents. En effet, s'ils sont conscients et formés correctement, il sera facile pour eux de détecter un incident et d'avertir rapidement les personnes référentes.

3. Maintenir un plan de réponse aux incidents

   Comme la plupart des démarches de sécurité, le plan de réponse a une approche d'amélioration continue. C'est pourquoi, lorsqu'un incident a eu lieu et qu'il a été traité, il est important de revenir sur le processus qui a été suivi durant le traitement de l'incident, afin d'en ressortir les avantages et les inconvénients pour améliorer les actions et procédures à mettre en place pour les prochains incidents.

Je propose ces mesures indépendamment de celles précitées pour la simple et bonne raison que j'estime que peu importe les risques, préparer un plan de réponses aux incidents est indispensable. Cela est particulièrement vrai dans un projet collaboratif tel que le LIMS étant donné qu'une grande part des risques n'est pas gérée par le département. Ce plan de réponse

va préparer le département à se protéger face aux éventuels incidents qui peuvent survenir dans le cas où les autres acteurs du projet ne font pas correctement leur travail.

10. Le plan de gestion du changement

Je vous avais présenté dans l'état de l'art le modèle de Lewin sur la gestion du changement. C'est un modèle qui est simple d'application et complet. Pour rappel, il se décline en trois phases :

- La phase de décristallisation
- La phase de transition
- La phase de recristallisation

Une gestion du changement est déjà prise en compte au niveau du projet global. Cependant, étant donné que chaque entité aura sa propre utilisation du LIMS, il est recommandé de définir sa propre gestion du changement, en accord avec celle déjà envisagée au niveau global.

Dans ce chapitre, j'aborderai la gestion du changement par rapport à la nouvelle gestion de la sécurité à mettre en place au sein du département analyse.

10.1. Phase de décristallisation

Cette phase a pour but de créer un sentiment d'urgence et un besoin de changement auprès des équipes du département, afin qu'ils adhèrent à la nécessité d'implémenter un nouveau LIMS. Ils utilisent déjà un LIMS, qui a les fonctionnalités nécessaires pour leur permettre de faire leur travail. Il est donc nécessaire de les conscientiser sur les avantages d'utiliser un nouvel outil plus moderne et plus efficace, notamment en faveur de l'aspect collaboratif du LIMS.

Il est tout aussi important de les préparer aux nouveaux comportements à adopter que cela va engendrer. Ils doivent être conscientisés sur la valeur de leurs actifs essentiels, afin de leur donner l'envie de les protéger et donc de s'impliquer dans la sécurité, même si cela ajoute des tâches supplémentaires à ce qu'ils ont à faire.

Pour les aider dans cette prose de conscience, il faut apporter des preuves tangibles et concrètes à ce qu'on leur dit. Cela peut se faire de différentes manières :

- En communiquant avec eux, par le biais de newsletter, de mails informatifs, en partageant des articles de journaux sur le sujet, … ;
- En réalisant des workshops : pourquoi ne pas leur montrer une cyberattaque fictive durant laquelle ils pourront se rendre compte de la facilité qu'ont certains attaquants à pénétrer des systèmes, et des différentes manières par lesquelles un utilisateur peut, sans s'en rendre compte, ouvrir la porte à des attaquants.

Cette étape est cruciale, car elle va permettre de mettre en lumière les résistances face aux changements, qui seront traitées lors de la phase suivante. La phase de décristallisation doit

commencer sans plus attendre étant donné l'avancement que le projet LIMS a déjà au sein de Solvay. Normalement, cette phase est censée débuter avant l'implémentation d'un nouveau projet.

10.2. Phase de transition

Cette phase est la plus longue. Elle s'étend sur l'ensemble de l'implémentation du projet. Dans notre cas, ce sera tout au long de la mise en place des différentes mesures précédemment présentées.

Cette phase permettra d'atteindre l'objectif final défini. Il est intéressant de définir cet objectif avec les utilisateurs, afin de les impliquer totalement dans le projet et d'obtenir leur adhésion. C'est donc lors de cette phase que je conseille d'appliquer les mesures présentées plus haut concernant les utilisateurs. Pour chaque mesure mise en place, où bénéfice apporté, il est conseillé de le valoriser, afin de faciliter l'adhésion au changement.

10.3. Phase de recristallisation

Lorsque les mesures ont été mises en place et que les utilisateurs ont acquis les nouveaux comportements qu'implique la gestion de la sécurité, il est primordial de les ancrer dans les processus de l'entreprise pour éviter que les utilisateurs ne retombent dans leurs anciennes habitudes. L'implication des utilisateurs doit continuer même après que l'outil ait été mis en place. On peut faire cela en les responsabilisant et en les assistant, comme je l'ai proposé dans les mesures précédemment.

Partie 4 : Retour d'expérience

Réflexion sur la place du Business Analyst au sein d'un projet de sécurité

J'ai réalisé un stage en alternance de deux ans dans le département analyse de Solvay, durant lequel j'ai eu l'opportunité de travailler sur l'aspect sécurité du projet LIMS. Mon objectif était de comprendre ce qu'est la sécurité de l'information, et de comprendre l'outil qu'est le LIMS ainsi que l'usage qui devait en être fait afin de proposer des recommandations de mise en place du LIMS au département en tenant compte de tous ces paramètres. La sécurité est un sujet qui a été souvent abordé en cours durant mon master, mais qui n'a pas été approfondi dans les détails. C'est un vaste sujet qui, malgré sa complexité, concerne l'ensemble de notre société, tant au point de vue des entreprises que des particuliers. C'est pourquoi ce sujet a grandement suscité mon intérêt.

De manière générale, le business analyst représente le pont entre le business et l'IT. Son rôle est de comprendre les besoins du business, ses processus de fonctionnement et ses exigences en termes d'objectif dans le but de les traduire en langage informatique, de manière à en faciliter la compréhension pour l'IT. Le but final étant le développement d'un nouvel outil informatique adéquat répondant aux critères du business. De manière plus large, l'institut international des business analyst (IIBA) définit le business analyst comme étant la personne « responsable de découvrir, synthétiser et analyser l'information d'une grande variété de ressources de l'entreprise, ce qui inclus les outils, les processus, la documentation et les parties prenantes » (BABOK, 2015, p. 2).

Par ailleurs, le règlement général de la protection des données (RGPD) consacre le principe de « security by design », qui impose aux entreprises d'intégrer la sécurité dès la conception d'un projet au niveau du traitement des données personnelles. Cette démarche repose sur la réalisation d'une analyse de risques spécifique aux données personnelles, afin de dégager les impacts qu'un mauvais traitement de celles-ci peut engendrer sur l'organisation (Ejzyn et Van den Berghe, 2018).

Je pense que ce principe doit s'étendre à la sécurité de l'information de manière générale. A travers cette mission, j'ai pu me rendre compte de l'importance que représente l'aspect sécurité dans la mise en place d'un outil informatique. Ma mission était d'autant plus complexe qu'il s'agissait d'un outil déjà partiellement implémenté au sein du groupe Solvay. Intégrer des principes de sécurité après la conception d'un projet impose des changements inévitables, ce qui engendrera des coûts supplémentaires pour l'organisation concernée par le projet. Toutes ces raisons justifient d'intégrer la sécurité dans les projets d'un business analyst.

Je n'ai pas trouvé de source littéraire abordant ce point de vue, cependant, j'ai eu l'occasion de m'entretenir avec Xavier Paulus, membre du groupe sécurité Solvay, et Guillaume Collard, expert en risques digitaux pour Solvay, à propos du projet LIMS et tous deux sont unanimes : le projet LIMS n'a pas été conçu en prenant en compte les risques sécurité de manière

suffisante. Ils sont conscients du retard de Solvay concernant la sécurité de l'information au sein du groupe. C'est pourquoi une révision totale de ses politiques de sécurité est en cours. Ce point est abordé dans le présent travail.

En conclusion, le métier de business analyst est très vaste, et c'est ce qui me plait : les sujets qu'on peut traiter sont nombreux et toujours plus enrichissants.

Réflexion sur ma méthodologie et la formation de Business Analyst

Combiner un stage en alternance avec la réalisation d'un mémoire n'est pas chose facile. En effet, avec un stage aussi prenant, et demandant autant de responsabilités, se plonger de manière approfondie dans la rédaction d'un mémoire est extrêmement compliquée. La crise sanitaire et l'impact psychologique qu'elle engendre ainsi que l'obligation de se confiner et donc d'être enfermé chez soi a été par moment un obstacle à la motivation et à l'inspiration. De plus, l'éloignement de l'établissement universitaire a créé un fossé quant à ma sensation d'être encore étudiante. Le timing prévu à la réalisation de ce mémoire a donc été compliqué à respecter.

La formation de Business analyst induit le sujet de sécurité de l'information. Cela dit, même si nous avons souvent abordé le sujet de la sécurité de l'information, me lancer dans la rédaction d'un mémoire sur ce sujet a été un réel défi, sachant que je n'avais que très peu de connaissances en la matière. J'ai cependant eu la chance d'être accompagnée et conseillée par mon promoteur, expert en sécurité. C'est un sujet vaste et fascinant, qui impose cependant une régularité dans son apprentissage étant donné que, et nous l'avons vu, c'est un sujet qui évolue rapidement.

Réaliser des entretiens avec des experts du domaine ainsi que des acteurs du projet est indispensable. Cependant, les réaliser avant la finalisation de la partie contextualisation de ce travail n'est pas idéal. En effet, en avançant dans la rédaction de cette partie de mon mémoire, je me suis rendu compte qu'il me manquait certaines informations que j'aurais pu obtenir si j'avais réalisé mes entretiens après la finalisation de cette partie. Heureusement, j'ai la chance d'être entourée de personnes au sein du groupe Solvay, et qui m'ont été d'un grand soutien et n'ont jamais hésité à me répondre lorsque j'avais des questions supplémentaires à leur poser, même après avoir eu un entretien avec eux.

La réalisation de ce mémoire sur le sujet de la sécurité de l'information ainsi que la mission qui m'a été confiée durant mon stage m'ont permis de mettre en pratique un grand nombre de compétences que le master nous a enseignées :

- Analyser et modéliser : j'ai dû analyser l'organisation, le projet initial et modéliser le fonctionnement de l'outil LIMS pour comprendre et déceler les différents actifs essentiels afin de réaliser une analyse de risques pertinente ;
- Participer à la stratégie de gouvernance : Solvay ayant le souhait de maintenir une cohérence pour l'entièreté de ses entités au niveau de la sécurité de l'information, j'ai

dû la comprendre afin de la prendre en compte dans la solution que j'ai proposée au département analyse ;
- Gérer un projet : la compréhension d'un business et la réalisation d'une analyse de risques sont des éléments clés faisant partie intégrante d'une gestion de projet ;
- Collaborer : la collaboration avec les différents acteurs du projet LIMS a été indispensable. Elle s'est effectuée au travers d'entretiens permettant de comprendre le fonctionnement de l'entreprise et du nouveau LIMS mais également les manquements et besoins en termes de sécurité de l'information.

Il s'agissait de ma première analyse de risques, et, bien que le sujet soit complexe, j'y ai pris part avec beaucoup d'intérêt. La mécanique est logique à partir du moment où on l'a comprise. Mon analyse est certes non exhaustive et avec le recul, je pense que j'aurais pu aller encore plus loin afin d'être plus complète. J'ai également le sentiment que mes recommandations sont encore un peu naïves, à cause de mon manque d'expérience en la matière. Je reste cependant convaincue que cette analyse de risques pourrait servir de base solide au département analyse de Solvay ainsi que la méthodologie que j'ai proposée. La pratique m'aidera à améliorer mes compétences en matière de réalisation d'analyses de risques, et cela donnera lieu à des recommandations toujours plus pertinentes.

Conclusion

Ce travail avait pour objectif de répondre à la question suivante : « Comment assurer la sécurité de l'information dans la mise en œuvre d'un outil collaboratif au sein du groupe Solvay ? », et d'accompagner le département analyse de Bruxelles, futur utilisateur de cet outil collaboratif, dans la mise en place des bonnes pratiques pour garantir la sécurité de son information.

Pour atteindre ces objectifs, j'ai divisé ce travail en trois parties. J'ai commencé par l'étude de l'art, en me référant à la littérature et aux avis d'experts afin de développer ma connaissance sur le sujet. Pour adapter cette connaissance au cas de Solvay, j'ai par la suite étudié le fonctionnement du groupe en matière de gestion de projet, ainsi que celui du nouveau LIMS à implémenter, dans le but de réaliser une analyse de risques pertinente pour les besoins du département. Pour terminer, grâce à tout cela, j'ai pu proposer des recommandations appropriées qui aideront le département à atteindre ses objectifs.

Grâce à l'étude de l'art, j'ai pu mettre en évidence les grands principes à respecter pour garantir la sécurité de l'information : la disponibilité, l'intégrité et la confidentialité de celle-ci. J'ai pu également constater que de nombreuses menaces pèsent sur la sécurité de l'information, révélant les deux grands enjeux de la sécurité : l'enjeu technique et l'enjeu humain. Afin de contrôler ces enjeux, j'ai pu proposer, en me basant sur la norme ISO 27000, une démarche de gestion de sécurité de l'information afin de l'inclure dans un projet concret. Ceci m'a appris que pour gérer un projet sécurité, l'approche par gestion des risques est la plus pertinente.

Suite à ces recherches, l'analyse des processus existant du département analyse de Bruxelles, j'ai pu souligner le manque de maturité en termes de sécurité de l'information. En analysant l'existant en matière de sécurité au sein de l'ensemble du groupe Solvay, ainsi que le fonctionnement du nouveau LIMS, j'ai pu proposer une adaptation de la politique de sécurité du groupe au département, et élaborer une liste de risques auxquels il fait face. S'en est suivie une analyse de risques, utilisant une méthode simplifiée mise en place par le Fedict, qui a permis d'élaborer dix mesures de sécurité qui permettront au département analyse de se protéger des différents risques précédemment listés.

Étant donné qu'il est impossible pour une organisation de mettre en place en même temps toutes les mesures préconisées suite à une analyse de risques, il a fallu choisir et prioriser les mesures les plus pertinentes afin de les intégrer dans la rédaction d'un plan de sécurité pour le département.

L'étape suivante consiste pour le département à mettre en pratique les mesures prioritaires et d'y former ses équipes, sans oublier d'évaluer régulièrement et de faire évoluer cette sécurité, comme le suggère la démarche de gestion de sécurité suggérée par la norme ISO 27000. Ce travail pourra servir de référence pour mettre en place cela.

Pour rappel, ce travail concerne l'implémentation du nouveau LIMS, qui est prévue d'ici quelques semaines au sein du groupe Solvay. Cependant, ce travail pourra aussi servir

d'exemple au département afin qu'il se penche de manière approfondie sur les autres outils qu'il utilise, outils que j'ai rapidement abordé dans le cadre de ce travail. En effet, il est important que l'entièreté du système d'information soit sécurisé pour garantir une sécurité globale de l'information du département.

Bibliographie

Ouvrage

Cartau, C. (2018). *La sécurité du système d'information des établissements de santé.* France : Presses de l'EHESP.

Ejzyn, A. et Van den Berghe, T. (2018). *Cybersécurité et RGPD : protégez votre PME*. Limal : Anthémis.

IIBA. (2015). *BABOK - a guide to the business analyst body of knowledge*. Toronto : International Institute of Business analyst.

Articles de journal

A.F. (2020, 14 janvier). Des usines de Picanol victimes d'une cyberattaque : « Nous ne pouvon plus accéder à notre propre système ». *RTBF*. Récupéré de https://www.rtbf.be/info/economie/detail_des-usines-de-picanol-victimes-d-une-cyberattaque-nous-ne-pouvons-plus-acceder-a-notre-propre-systeme?id=10406577

Belga. (2020, 31 janvier). Cyberattaque visant Picanol – Picanol s'attend à un impact financier de moins d'un million d'euros. *Le soir*. Récupéré de https://www.lesoir.be/276828/article/2020-01-31/picanol-sattend-un-impact-financier-de-moins-dun-million-deuros

Bergerson, U. (2021, 4 février). Avec le télétravail vient la hausse des cyberattaques. *Le Devoir*. Récupéré de https://www.ledevoir.com/economie/594568/technologie-avec-le-teletravail-vient-la-hausse-des-cyberattaques

Henrion, S. (2020, 3 avril). L'importance du Cloud en cette période de confinement. *ProTime*. Récupéré de https://www.protime.be/fr-be/actualites/limportance-du-cloud-en-cette-periode-de-confinement

Mertens, J. (2021, 25 mars). La Belgique parmi les pays les plus ciblés par des cyberattaques. *Geeko Le Soir*. Récupéré de https://geeko.lesoir.be/2021/03/25/la-belgique-parmi-les-pays-les-plus-cibles-par-des-cyberattaques/

Rapport

ANSSI. (s.d.). *EBIOS Risk manager*. France : ANSSI. Récupéré de : https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

IBM Security. (2021). *X-Force Threat Intelligence Index*. New-York : IBM Corporation. Récupéré de https://www.ibm.com/downloads/cas/M1X3B7QG

Sécurité Sociale. (2017). *Sécurité et confidentialité de l'information Définitions*. Belgique : Sécurité Sociale. Récupéré de https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/mnm_def_definitions.pdf

Solvay. (2018). *Rapport Annuel Intégré*. Bruxelles : Solvay. Récupéré de https://www.solvay.com/sites/g/files/srpend221/files/2019-04/Solvay%20Rapport%20Annuel%20Int%C3%A9gr%C3%A9%202018%20pdf%20version%20digitale.pdf

Solvay. (2020). *Rapport annuel*. Bruxelles : Solvay. Récupéré de http://main.solvay.acsitefactory.com/sites/g/files/srpend221/files/2021-03/Solvay%202020%20Rapport%20annuel.pdf

Saraydaryan, J. (s.d.). *Management du risque*. Lyon : CPE. Récupéré de https://jacques-saraydaryan.github.io/assets/pdf/courses/Security-Risk-r4.pdf

Documents internes

Département Analyse Solvay. (2020). *Manuel qualité* [Intranet]. Bruxelles : Solvay.

Département Analyse Solvay. (2019, 15 mars). *Politique qualité* [Intranet]. Bruxelles : Solvay.

Huet, A. (2019). *Sécurité de l'information et gestion du risque*. [PDF]. Bruxelles : InfoSafe.

ISO. (2008). ISO/IEC 27005:2008 Annex C & D. ISO/IEC 2008.

Solvay. (2021). *Information and Cyber Security Policy* [Intranet]. Bruxelles : Solvay.

Sites internet

ANSSI. (2021). *Principales menaces*. Récupéré le 12 mars 2021 de https://www.ssi.gouv.fr/entreprise/principales-menaces/

Autorité de protection des données. (2021). *Une politique de sécurité de l'information*. Récupéré le 12 mars 2021 de https://www.autoriteprotectiondonnees.be/professionnel/themes/securite-de-l-information/une-politique-de-securite-de-linformation

BPMS. (s.d.). *Méhari / Gestion des risques SSI*. Récupéré le 8 mai 2021 de https://www.bpms.info/mehari-gestion-risques-ssi/

CaixaBank. (2021). *Qu'est-ce que le logiciel malveillant RAT et pourquoi est-il si dangereux ?*. Récupéré le 21 mars 2021 de https://www.caixabank.es/particular/seguridad/quest-ce-que-le-logiciel-malveillant-rat-et-pourquoi-est-li-si-dangereux.html#

Cimelière, O. (2019, 8 avril). *La réputation des entreprises menacées par les cyberattaques*. Récupéré le 10 mai 2021 de http://www.eclaireursdelacom.fr/la-reputation-des-entreprises-menacee-par-les-cyberattaques/

CNIL. (s.d.). *Le phishing, c'est quoi ?*. Récupéré le 24 mars 2021 de https://www.cnil.fr/fr/cnil-direct/question/le-phishing-cest-quoi

CNIL. (s.d.). *Sécurité : Tracer les accès et gérer les incidents*. Récupéré le 6 mai 2021 de https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents

E-Health. (s.d.). *Sécurité de l'information & GDPR*. Récupéré le 12 mars 2021 de https://www.ehealth.fgov.be/ehealthplatform/fr/securite-de-linformation-gdpr

E-Marketing. (s.d.). *Log (fichier)*. Récupéré le 5 mai 2021 de https://www.e-marketing.fr/Definitions-Glossaire/Log-fichier-238242.htm

ISO (s.d.), *L'exploration spatiale à son apogée.* Récupéré le 3 mai 2021 de https://www.iso.org/fr/home.html

Jumpsec. (2021, 31 mars). *Why attackers don't care about your lists of vulnerabilities*. Récupéré le 2 avril 2021 de https://www.jumpsec.com/insights/why-attackers-dont-care-about-your-lists-of-vulnerabilities/

Krumrey, N. (2020, 8 octobre). *Guide de la gestion des logs et de l'importance de la journalisation*. Récupéré le 5 mai 2021 de https://www.logpoint.com/fr/blog/gestion-des-logs/

Latto, N. (2020, 20 février). *Qu'est-ce que la cybercriminalité et comment vous en préserver ?*. Récupéré le 22 avril 2021 de https://www.avast.com/fr-fr/c-cybercrime#topic-1

ManagerGO. (2021, 29 mars). *Managez le changement en 3 étapes selon le modèle de Lewin*. Récupéré le 7 mai 2021 de https://www.manager-go.com/gestion-de-projet/le-changement-par-lewin.htm

Milkovich, D. (2020, 23 décembre). *15 Alarming Cyber Security Facts and Stats*. Récupéré le 2 avril 2021 de https://www.cybintsolutions.com/cyber-security-facts-stats/

MONARC cases. (2021). *What is MONARC ?*. Récupéré le 8 mai 2021 de https://www.monarc.lu/

Ravet, E. (2020, 27 octobre). *La sécurité des applications web : un enjeu majeur pour les entrreprises*. Récupéré le 1 avril 2021 de https://www.scalair.fr/blog/la-securite-des-applications-web-un-enjeu-majeur-pour-les-entreprises

Solvay. (2021). *Find the right solutions for your needs*. Récupéré le 15 mai 2021 de https://www.solvay.com/en/

WestStar. (2021). *BEC Attacks : What They Are and How To Protect Yourself*. Récupéré le 21 mars 2021 de https://www.weststarbank.com/our-info/bec-attacks--what-they-are-and-how-to-protect-yourself

Complétements bibliographiques

Axys Consultants. (2019, 30 septembre). *Pourquoi y a-t-il résistance au changement ?*. Récupéré le 7 mai 2021 de https://www.axys-consultants.com/blog/transformation-digitale/pourquoi-resistance-changement

Beky, A. (2021, 25 mars). Stephan Hadinger (AWS France) : « La sécurité cloud, c'est une responsabilité partagée ». *Silicon*. Récupéré de https://www.silicon.fr/hadinger-aws-securite-cloud-responsabilite-partagee-403481.html

Centre for cyber security Belgium. (s.d.). *Cybersécurité Guide de gestion des incidents*. Bruxelles : Cyber Security Coalition. Récupéré de https://ccb.belgium.be/fr/document/cyber-security-incident-management-guide

CLUSIF. (2011). *Gestion des incidents de sécurité du système d'information (SSI)*. Paris : CLUSIF. Récupéré de https://clusif.fr/wp-content/uploads/2015/09/clusif-2011-gestion-des-incidents.pdf

INCH. (2015). *Débat : le changement est-il toujours une bonne chose ?*. Récupéré le 7 mai 2021 de https://www.ineos.com/fr/inch-magazine/articles/issue-8/debat-le-changement-est-il-toujours-une-bonne-chose-/

Ivision. (2018, 18 décembre). *Mettre en place une politique de sécurité informatique : les bonnes pratiques*. Récupéré le 16 mars 2021 de https://www.ivision.fr/mettre-en-place-une-politique-de-securite-informatique-les-bonnes-pratiques/

Les Echos. (2016, 10 février). Le « risk appetite » : une nouvelle dimension de la gouvernance des entreprises ?. *Les échos*. Récupéré de http://archives.lesechos.fr/archives/cercle/2016/02/10/cercle_151586.htm

Loriau, N. (2020). *Réseau et sécurité*. Syllabus. ECAM, Bruxelles

Michalle, P. (2021, 10 mai). Cybercriminalité, des comportements à changer pour survivre dans la jungle informatique. *RTBF*. Récupéré de https://www.rtbf.be/info/belgique/detail_cybercriminalite-des-comportements-a-changer-pour-survivre-dans-la-jungle-informatique?id=10758997&fbclid=IwAR31nbOx-mqZyWlBFssysTk6RYDMTL8xRblBk7CRPWDTgAy_IKoYkRYxpt0

Nguyen, T. (2020). *22BA040 – Stratégie et gouvernance TIC*. Syllabus. ICHEC, Bruxelles.

Nollevaux, G. (2017). *Gestion de projets informatiques, Gestion de projets digitaux*. Syllabus. ICHEC, Bruxelles.

Smith, C. (2018, 17 octobre). Battle of change theoris : Lewin Change Management Model vs. Kotter 8 step Process. *Change*. Récupéré de https://change.walkme.com/lewin-change-management-model/

Glossaire

AODOCS : outil de gestion documentaire de la suite Google largement utilisé au sein du département analyse de Bruxelles.

Cyberattaque : signifie une attaque qui est réalisée sur un dispositif informatique via un réseau.

LAN = Local Area Network

Malware = Logiciel malveillant

PDCA = Plan-Do-Check-Act : abréviation utilisée lorsqu'on fait référence à la roue de Deming

Péroxyde[2] : *composé chimique renfermant une plus grand quantité d'oxygène qu'un oxyde normal.*

Polymères spéciaux : *plastiques de qualité supérieure, avec des meilleures propriétés mécaniques, une meilleure stabilité thermique et chimique*.

RIC = Research and Innovation Corporate : abréviation utilisée qui fait référence à une entité de la fonction Recherche et Innovation.

Shared Drive Google : fonctionnalité propose par Google qui permet de gérer un Google drive avec plusieurs personnes sans que les documents ne soient liés à un utilisateur spécifique.

VPN = Virtual Private Network

WAN = Wide Area Network

[2] Les mots en italiques sont des définitions de termes scientifiques issus d'encyclopédies scientifiques. N'étant pas compétente dans la chimie, je ne sais pas expliquer ces termes complexes.