Mémoire de fin d'études

Année 2022-2023

COMMENT INTÉGRER UN SMSI AU SEIN D'UNE TPE/PME ?

Présenté par :

Mickaël SAMPAIO

Réalisé dans le cadre de mon Master Networks and Security Manager à l'Efrei

En apprentissage chez PHILIANCE Formation

Remerciements

Je tiens à remercier mon tuteur Julien DAVROUX qui pendant ces 3 ans m'a fait confiance pour la mise en place de nombreuses solutions techniques.

Je remercie Patrick TESSIER pour m'avoir accepté en apprentissage au sein de son entreprise familiale ce qui m'a permis de développer de nombreuses compétences pendant ces trois années d'apprentissage.

Je remercie Émilie TESSIER pour sa bienveillance et sa patience, et qui m'a donné la chance de pouvoir prouver ma valeur dans un cadre de travail serein.

Je remercie tous les intervenants de l'Efrei qui nous ont fait étudier des concepts tout autant complexes qu'intéressants.

Enfin, je remercie l'ensemble de mes collègues de PHILIANCE Formation qui m'ont permis de grandir et de prendre confiance en moi.

Table des matières

Glossaire

SI : Système d'Information, est un ensemble de ressources et de dispositifs permettant de collecter, stocker, traiter et diffuser les informations nécessaires au fonctionnement d'une organisation.

SMSI : Système de Management de la Sécurité de l'Information, est un ensemble de politiques, de documents, et de méthodes visant la gestion de la sécurité de l'information.

PSSI : Politique de Sécurité du Système d'Information, La politique de sécurité des systèmes d'information est un plan d'action défini pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information.

FAI : Fournisseur d'Accès Internet, est un organisme offrant une connexion à Internet, le réseau informatique mondial.

EDR : Endpoint Detection Response, est une solution de sécurité des terminaux qui inclut la surveillance en temps réel et la collecte des données de sécurité des terminaux avec un mécanisme de réponse automatisée aux menaces.

IDS : Intrusion Detection System, est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée. Il permet ainsi d'avoir une connaissance sur les tentatives réussie comme échouées des intrusions.

IPS : Intrusion Prevention System, est un outil des spécialistes en sécurité des systèmes d'information, similaire aux systèmes de détection d'intrusion, permettant de prendre des mesures afin de diminuer les impacts d'une attaque.

PCA : Plan de Continuité d'Activité, a pour objet de décliner la stratégie et l'ensemble des dispositions qui sont prévues par une organisation pour garantir la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal.

PRA : Plan de Reprise d'Activité, constitue l'ensemble des procédures documentées permettant de rétablir et de reprendre les activités en s'appuyant sur des mesures temporaires adoptées pour répondre aux exigences métier habituelles après un incident

SIEM : Security Information and Event Management, est une solution de sécurité qui permet aux organisations de détecter les menaces avant qu'elles ne perturbent leurs activités.

Mémoire ECC : Une mémoire ECC (Error-Correcting Code) est un type de mémoire vive avec un code correcteur permettant de détecter et de corriger les types les plus courants de corruption de données.

OS : Operating System, est un ensemble de programmes qui permettent le fonctionnement et l'utilisation des principales ressources de l'ordinateur

ROI : Return On Investment, désigne un ratio financier qui mesure le montant d'argent gagné ou perdu, par rapport à la somme initialement investie dans un investissement.

SPOF : Single Point Of Failure, est un point d'un système informatique dont le reste du système est dépendant et dont une panne entraîne l'arrêt complet du système.

IT : Information Technology, appelée aussi système informatique, désigne le domaine technique du traitement de l'information, souvent dans un contexte professionnel.

DICT : Disponibilité, Intégrité, Confidentialité, Traçabilité, ce sont des indicateurs de sécurité utiles pour évaluer les besoins de sécurité associés à un actif.

SMCA : Système de Management de la Continuité d'Activité, est un système de gestion des risques qui regroupe le plan de continuité d'activité et le plan de reprise d'activité. Il est normalisé par la norme ISO 22301.

ITIL : Information Technology Infrastructure Library, est un ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information.

PII : Personal Identifiable Information, sont des ensembles de données qui peuvent être utilisées pour distinguer un individu spécifique.

PDCA : Plan Do Check Act, qui peut se traduire par Planifier, Déployer, Contrôler, Agir, est une méthode d'amélioration continue qui présente 4 phases à enchaîner de manière itérative pour améliorer un fonctionnement existant

KPI : Key Performance Indicator, est un indicateur utilisé pour l'aide à la décision dans les organisations. Les KPI sont utilisés particulièrement en gestion de la performance organisationnelle.

Introduction

Mon parcours

Je m'appelle Mickaël SAMPAIO, étudiant en Master Network & Security Manager, et c'est dans le cadre de ce Master que j'ai rédigé ce mémoire de fin d'étude, qui découle de quatre années d'apprentissage, dont trois dans l'organisme de formation privé PHILIANCE.

J'ai pu pendant ces trois dernières années, assister mon tuteur dans diverses mises en place technique pour répondre aux besoins des cursus de formations et aux besoins des différents collaborateurs et services internes. Et j'ai eu pour responsabilité de mettre en place une plateforme pour gérer les processus interservices.

C'est également dans cette même entreprise que j'ai proposé un projet d'intégration d'un SMSI, et que j'ai eu la responsabilité de celui-ci.

Pendant cette période, j'ai découvert mon véritable intérêt pour la gestion de la sécurité. J'ai également découvert que j'appréciais avoir une vision d'ensemble d'une organisation, de toutes les relations entre les différents services, et un fort attrait pour le développement d'infrastructures durables.

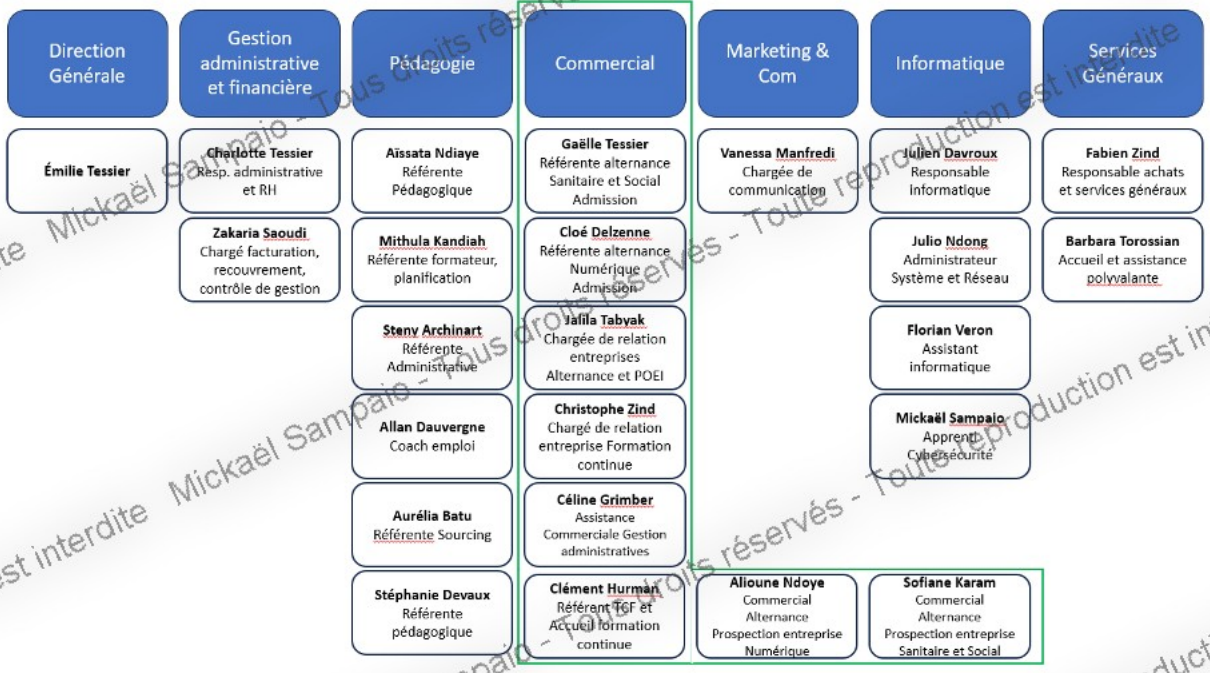
L'organisme de formation PHILIANCE

J'effectue mon apprentissage au sein de PHILIANCE. PHILIANCE est un organisme de formation, principalement dans le domaine du numérique, qui s'est vu croître promptement pendant ces dernières années à la suite de la crise sanitaire du COVID 19.

En effet, en l'espace de 3 ans seulement, le nombre de collaborateurs est passé de cinq à plus d'une vingtaine, et le nombre de cursus de formation est passé d'une moyenne annuelle de cinq à une trentaine.

C'est à la suite de ce fort développement que le groupe EUREKA a racheté PHILIANCE, voyant en cet organisme un sérieux potentiel.

Organigramme



PHILIANCE compte 24 collaborateurs répartis sur divers services :

- La Direction Générale est représentée par Émilie Tessier.
- Le service Gestion administrative et financière, qui s'occupe donc de tout l'aspect administratif et financier interne.
- Le service Pédagogie, où on retrouve une gestion administrative mais qui est dédié à la gestion des cursus. On y trouve également les coachs emploi, la référente planification des cursus, etc…
- Le service Commercial, où on trouve les référentes admissions, les chargés de relation entreprise.
- Le service Marketing & Communication contient une seule collaboratrice qui s'occupe de toutes les productions visuels et graphiques de PHILIANCE et qui s'occupe des réseaux sociaux.
- Le service Informatique, auquel j'appartiens et où nous gérons tout l'aspect sécurité IT, l'assistance informatique, et les projets IT internes.
- Les services généraux, qui s'occupe de l'accueil principal et des divers achats et locations.

Problématique

Pendant ces trois années passées au sein du même organisme, et étant le premier collaborateur embauché juste avant le fort développement de PHILIANCE, j'ai pu constater différentes problématiques que peut rencontrer une récente TPE qui subit une forte croissance.

Le mot subir peut paraître mal approprié au premier abord, mais c'est bel est bien le cas. Initialement, la gestion de l'entreprise était très minimaliste : processus internes inexistant, pas de développement stratégique, chacun des cinq collaborateurs travaillaient ensemble et traitaient quasiment tous les mêmes sujets de manière indépendante.

J'ai donc pu voir l'entreprise travailler d'une manière où quand se présentait une barrière, que cette barrière soit administrative, une faille dans la gestion d'un cursus, un incident informatique, ou autre, on trouvait une solution in extremis et on passait à la suite.

Or cette gestion, où on attend qu'un incident fasse son apparition pour devoir trouver une solution, ne peut pas répondre aux besoins d'une entreprise qui maintenant détient plusieurs services bien distincts, avec différents acteurs répondant de rôles et de fonctions bien spécifique.

Il est évident qu'un organisme gérant plusieurs dizaines de cursus se verrait perdre des bénéfices de manière significative si son SI venait a ne plus être disponible, si un audit de conformité réglementaire venait à ordonner la mise en réglementation avant la reprise des activés ou autre.

Et cette rapide croissance de PHILIANCE n'a pas laissé le temps de poser des bases solides en termes de sécurité, que ce soit réglementaire, sécurité du SI, ou même simplement de sécurité physique.

En effet, pendant la période où PHILIANCE est passé de cinq collaborateurs à une vingtaine, chacune des mises en place ont été pour répondre à un besoin immédiat, et aucun investissement n'a été envisagé pour ce qui est de la sécurité ou de la qualité.

L'entreprise a maintenant atteint un niveau presque stable et il selon moi impératif de rapidement poser des bases solides et durables avant d'envisager tout autre développement ou changement d'axe stratégique.

C'est pourquoi j'ai proposé à la Direction de gérer un projet de mise en place d'un SMSI pour répondre aux besoins actuels et urgents de l'organisme, d'où la problématique que je vais présenter dans ce mémoire :

Comment mettre en place un Système de Management de la Sécurité de l'Information dans une TPE/PME ?

Découpage du mémoire

Ce mémoire se découpera en plusieurs sections, à savoir 6 parties :

- Les raisons et justifications de ma problématique.
- L'état de l'art où je vous présenterai mes recherches qui m'ont guidé au déploiement du SMSI.
- Le cadrage du projet où je décris le périmètre et les ressources du projet.
- L'étude fonctionnelle où je me suis aidé, par le biais de différentes méthodes, à concentrer le projet sur une catégorie spécifique de la sécurité.
- L'étude technique où j'explique comment j'ai déployé les documents et mesures de contrôles nécessaires à l'application de la sécurité.
- Le compte-rendu du projet et les bilans professionnel et personnel que j'ai tiré de celui-ci.

Problématique

Description de la problématique

Je fais donc partie du service informatique de PHILIANCE, et compte tenu de mon parcours scolaire et du Master que je suis, j'ai eu l'initiative de proposer la mise en place d'un SMSI pour répondre aux besoins actuels de sécurité chez PHILIANCE.

En effet, PHILIANCE dispense plusieurs cursus orientés dans le domaine du numérique. Et bien que les mœurs d'aujourd'hui sont tournés vers des cours en distanciels, nous continuons d'accueillir du publique pour des cours en présentiels.

De manière générale, l'activité de PHILIANCE présente plus de vulnérabilités que la plupart des autres entreprises du secteur tertiaire.

Accueillir un public c'est :

- Prendre le risque de dégradation ou de vol physique de matériel
- Prendre le risque d'attaque malveillante sur le SI (d'autant plus que le public accueilli est plus ou moins adepte aux techniques de cyberattaques)
- Prendre le risque qu'un utilisateur pratique une activité illégale

Gérer un cursus c'est :

- Traiter massivement des données personnelles et plus ou moins confidentielles
- Proposer et exposer divers services internes à des personnes dont on n'a pas forcément confiance
- Transmettre ou recevoir des données avec des partenaires, souvent du service public et particulièrement ciblés par des cyberattaques.

De plus, pour répondre aux besoins de gestion massive des apprenants et des cursus, PHILIANCE utilise diverses applications externes qui mène à une externalisation des données sur diverses plateformes, ce qui mène à d'autres risques et questionnements :

- Que faire en cas de fuite de données sur une de ces plateformes ?
- Comment s'assurer que la plateforme est sécurisée ?
- Quelles sont les politiques de confidentialité ?
- Où sont stockés les données, et donc sous quelles réglementations les données sont soumises ?

À cela s'ajoute un facteur particulièrement important, le système informatique est très peu sécurisé :

- Il n'y pas de pare-feu autre que celui du modem du FAI.
- Il n'y pas de cloisonnement réseau mis à part qu'il y a un réseau distinct pour la formation et un second réseau pour les internes.
- Il n'y a pas de SIEM.
- Il n'y a pas de serveur antivirus ou d'EDR.
- Il n'y a pas d'IDS ou d'IPS.
- Il n'y a pas de station blanche pour analyser les médias amovibles alors que ceux-ci sont régulièrement partagés.
- Il n'y a pas de planification de sauvegarde correctement définie.
- Il n'y a pas de Proxy Web
- Pour finir, il n'y a aucun PCA ni PRA définis.

Mais le système d'information ne comprend pas uniquement le système informatique, il comprend également l'organisation dans son ensemble, ces processus, ces ressources humaines, à savoir les collaborateurs mais également les formateurs et tout prestataires externes et partenaires.

Et il n'y pas non plus de mesure engagée visant à former ou simplement sensibiliser sur les principes fondamentaux de la sécurité.

Il est clair que face à ces potentiels risques et en faisant une très brève analyse de l'existant en termes de sécurité, n'importe qu'elle personne avertie sur les problématiques en matière de sécurité tirerait la sonnette d'alarme.

Et c'est ce que j'ai fait en soumettant le projet de développer un SMSI au sein de PHILIANCE, l'objectif étant de minimiser chacun des risques.

Les causes de ma problématique

En faisant une cartographie des risques, je pourrais estimer le niveau de risque globale de PHILIANCE. L'objectif étant de réduire ce niveau de risque globale de manière significative avec le SMSI.

De plus, le manque de cartographie des processus, et ceux-ci changeant régulièrement, il est régulier qu'une donnée traitée soit stockée sous différents formats et sous différents médias.

Par exemple, quand un collaborateur doit traiter une donnée qu'il reçoit par mail, il n'est pas rare qu'une sauvegarde soit réalisée sur son bureau, puis sur un dossier partagé, multipliant les niveaux de risques si le poste du collaborateur venait à être compromis.

Cependant, intégrer un SMSI au sein de PHILIANCE sera un projet lourd, et il me faut donc l'adapter selon les possibilités pour faire en sorte que la conduite du changement se passe du mieux possible.

Pour résumer

Pour mener à bien le projet, il faut donc que je prenne en compte l'activité globale de l'entreprise, et avoir une vision extrêmement large de tout ce qui entre en compte dans la sécurité.

On pourrait penser au premier abord qu'il n'est pas utile de comprendre comment le collaborateur A interagit avec le collaborateur B tant que leurs postes de travail sont sécurisés et sauvegardés. Or, comprendre le but d'une interaction, les processus dont découlent l'opération, et identifier les actifs en jeu, permet de bien mieux identifier les risques.

Globalement, je vais donc devoir :

- Comprendre l'activité de l'organisme dans son ensemble.
- Estimer le retour sur investissement d'une telle mise en place.
- Convaincre la Direction des bénéfices et de la nécessité d'adopter une culture de sécurité.
- Estimer le budget nécessaire pour répondre aux différents besoins.
- Planifier le projet.
- Réaliser une analyse de l'existant, que ce soit en termes d'actifs ou organisationnels.
- Classifier les données.
- Élaborer une politique de sécurité qui détaille les principes, les règles et les responsabilités liés à la sécurité de l'information dans l'entreprise.
- Définir les responsabilités de chacun.
- Cartographier les processus.
- Identifier, évaluer et traiter les risques liés à la sécurité de l'information.

- Définir les Plans de Continuité d'Activité (PCA) et Plans de Reprise d'Activité (PRA).
- Proposer les méthodes techniques de sécurité en adéquation avec les besoins.
- Définir les procédures d'incident pour réagir rapidement et efficacement en cas d'incident de sécurité.
- Respecter les exigences légales et réglementaires pour assurer la conformité réglementaire du SMSI.
- Établir un document de revue continue pour revoir et ajuster régulièrement le SMSI et s'assurer qu'il reste efficace face aux nouvelles menaces et aux changements dans l'entreprise.

Analyse de l'existant

Locaux

PHILIANCE possède deux locaux distincts et loue deux salles dans un troisième local.

PHILIANCE est basé au 2 rue Jean Mermoz à Évry-Courcouronnes en Ile-de-France, c'est dans ce bâtiment que travaille l'intégralité des internes et où environ la moitié des cours sont dispensés.

Il y a deux salles de cours dans un local à Créteil où l'accès internet est fournis par le propriétaire.

Et enfin un local au Parc Élysée également à Évry-Courcouronnes où sont dispensé des cours.

Matériels

PHILIANCE possède environ 150 postes de travails, tour et ordinateurs portables confondus

3 modems FAI, deux au bâtiment Jean Mermoz pour fournir l'accès à internet aux collaborateurs et aux apprenants et formateurs. À noter qu'une box est entièrement dédiée à l'interne, la seconde est dédiée à la formation. Enfin le troisième modem est situé au Parc Élysée pour l'accès internet aux apprenants et formateurs.

6 bornes WiFi au bâtiment Jean Mermoz pour fournir l'accès à internet par WiFi.

6 switches Cisco qui desservent les salles de formations et les serveurs

10 téléphones IP

2 smartphones

Applicatifs et solutions logicielles

Interne :

- 6 lignes VOIP chez Orange, avec une gestion de la téléphonie IP sur le modem.
- Serveur* de sauvegarde VEEAM sous Windows 10 20H2
- Serveur* de partage de dossier Samba sous Debian 11
- Serveur* VPN Wireguard sous Debian 11
- Serveur* CRM CoRM sous Ubuntu 14.04

* Ce sont des tours classiques qui n'ont pas forcément un hardware ou BIOS adapté à une utilisation en tant que serveur d'entreprise (pas de mémoire ECC, de redondance hardware, etc…)

En externe, nous avons 4 lignes VOIP chez OVH avec une gestion sur une plateforme externe

Plateformes et services web

PHILIANCE utilise diverses plateformes Web qu'il ne faut pas mettre de côté dans la prise en compte des risques, car nous téléversons des diverses données dans ces plateformes qui ne nous appartiennes pas.

Il faut donc que je liste les principaux services et plateformes web que nous utilisons :

- Digiforma, une plateforme de gestion de formation.
- Gandi, un fournisseur de service cloud.
- Notion, un outil pour réaliser des documentations de manière collaborative.
- Google Workspace, une suite d'outils collaboratif équivalent à Microsoft 365.
- Discord, un logiciel de communication communautaire.
- Zoom, un logiciel de visioconférence.
- Et enfin Educentre, qui est une plateforme de gestion de cursus et qui est en plein développement par un de nos partenaires.

Parmi tous ces services, je suppose que tous respectent les réglementations RGPD, cependant il faudra s'en assurer.

Néanmoins, je pense que seul Educentre qui est en plein développement par un de nos partenaires pourrait ne pas encore les respecter. Il faudra également s'en assurer, et le cas échéant, établir un contrat pour définir les responsabilités de PHILIANCE et de notre partenaire Xonatis dans le cadre du respects des réglementations quant aux données que nous téléversons sur cette plateforme.

Résumé

PHILIANCE a donc le strict minimum en termes de matériel qui plus est n'est pas forcément adapté aux besoins en termes de sécurité (services importants hébergés sur des ordinateurs classiques).

Du côté du réseau, la segmentation sur deux modems différents permet une première sécurité, mais n'est pas idéale. J'estime qu'il faudrait configurer une segmentation par VLAN et de la Haute Disponibilité.

Pour ce qui est des applications et solutions logiciels, je préconiserai des mises à jour régulières des OS et l'utilisation d'un seul fournisseur VOIP.

État de l'art

Rappel

La création d'un SMSI est une activité particulièrement lourde pour une TPE/PME. À cela s'ajoute que l'investissement pour la mise en place de sécurité de l'information n'est absolument pas prioritaire. Pour finir, je suis le seul collaborateur du service technique ayant fait des études dans le domaine de la sécurité informatique. Cependant, malgré de longues années d'études, je suis loin de pouvoir prétendre à mettre en place un SMSI. En effet, pour un tel projet, je suis obligé de combler certaines lacunes en matière de connaissances techniques et méthodologiques.

Je dois donc réaliser un état de l'art pour trois objectifs distincts :

- Apprendre ce qu'est un SMSI en profondeur.
- Convaincre de l'importance de l'investissement pour la mise en sécurité du SI.
- Adapter le SMSI pour une petite organisation et éviter que la mise en place soit trop lourde.

Sources et méthode de recherche

En premier lieu, j'ai besoin de développer mes connaissances sur qu'est un SMSI, comment le mettre en place, les méthodologies à appliquer.

Pour ce faire, j'ai accès à plusieurs ressources morcelées des standards ISO. Les standards ISO sont des normes internationales rédigées par une communauté d'experts mondiaux. La qualité de ces standards est indéniable et il est recommandé de se baser en premier lieu sur ceux-ci pour toutes types de recherches. Les standards ISO traitant de la sécurité de l'information et plus particulièrement de la mise en place d'un SMSI sont contenus dans la série ISO/IEC 27000.

Les standards ISO sont payants et sous copyright, cependant, je travaille dans un organisme de formation et nous offrons à nos apprenants un accès à une bibliothèque numérique en ligne, l'ENI, pour laquelle j'ai également un accès. Cette bibliothèque contient des cours se basant sur les standards ISO lié au management et à l'informatique.

De plus, il y a des ressources de qualités identiques qui sont publiées et accessibles gratuitement, les publications du NIST.

En second lieu, je dois effectuer des recherches sur l'état de la sécurité de manière globale, et surtout des cyberattaques, des attaques que subissent le plus les TPE/PME, et des pertes financières qui en découlent. Le but étant de conduire une réunion pour présenter les risques auxquels s'impose PHILIANCE et dont la Direction n'a pas forcément conscience.

Pour effectuer ces recherches, je vais devoir me baser sur des rapports d'organisme de sécurité informatique et des statistiques publiques.

Pour finir, je dois me renseigner sur les limites d'un SMSI dans un petit organisme. Le but étant d'adapter au possible la mise en place d'un projet aussi gargantuesque dans une petite entreprise. Cette recherche sera principalement orientée sur des retours d'expériences.

Première partie : Comment mettre en place un SMSI

Standards ISO

Pour effectuer mes recherches et découvrir en détail ce qu'est un SMSI, je me suis naturellement tourné vers les normes ISO de la série 27000. Et c'est plus particulièrement les ISO 27001 et 27002 qui permettent de guider à la démarche de la création d'un SMSI.

Mais tout d'abord je pense qu'il est important d'expliquer ce qu'est une norme ISO. Une norme ISO est une norme internationale qui est établit par des experts. Le but étant de décrire et de documenter un sujet en particulier pour définir la meilleure façon de faire.

Ces normes couvrent un éventail extrêmement large de sujets, mais toutes ont pour objectif de guider un organisme dans les règles de l'art sur une activité en particulier.

Le nom de l'organisme en français est "Organisation Internationale de Normalisation" et en anglais "International Organization for Standardization". Or aucune de ces abréviations ne donne "ISO". En effet, le but de cette organisation et des réunir des experts mondiaux, de toutes origines et de toutes cultures pour permettre de fusionner leurs expertises et leurs méthodes afin donc d'établir une norme qu'on peut donc qualifier, à juste titre, de la meilleure façon de faire. Dans cet esprit-là, l'organisme a préféré choisir un nom qui serait reconnu de tous sans pour autant se baser sur l'abréviation du nom de l'organisme dans une langue en particulier. Le nom "ISO" vient donc du terme dérivé "isos" qui en Grec veut dire "égal".

Il est donc effectivement cohérent, lorsqu'on veut effectuer une recherche pour combler des manques de connaissances, d'aller en premier lieu chercher s'il existe une norme ISO qui traite du sujet.

Parmi mes recherches, et étant très curieux, j'ai été naturellement dirigé vers différentes normes :

- ISO 9001 : c'est une norme qui vise à appliquer les bonnes pratiques en management de la qualité. Elle vise à guider les organismes dans leurs approches processus, les aide à s'engager dans une démarche d'amélioration continue de leurs processus, et est essentiellement centré sur la satisfaction client.
- ISO 31000 : c'est une norme qui vise à cadrer les organismes dans leur gestion des risques de manière globale, contrairement à l'ISO 27000 qui se concentre sur les risques liés à la sécurité de l'information.
- ISO 22301 : c'est une norme qui vise à guider les organismes dans la mise en place d'un SMCA, Système de Management de la Continuité d'Activité, qui regroupe un ensemble de méthodes et de documents tels que les PCA et PRA. Tout comme la norme ISO 31000, l'orientation de l'ISO 22301 n'est pas axée vers l'informatique mais est globale.

La série ISO 27000, plus correctement appelée ISO/IEC, est rédigée conjointement avec l'organisation ISO mais également avec la Commission Électrotechnique Internationale (IEC, pour International Electrotechnical Commission). Cette dernière apporte son expertise sur des sujets concernant l'électrotechnique, on peut par exemple penser à la bonne manière de réaliser et de vérifier un câblage physique. Néanmoins, afin d'éviter d'alourdir ce mémoire, j'évoquerai les standards ISO/IEC en raccourcissant leurs noms par standards ISO.

J'ai donc une base de standards ISO sur lesquels je peux me m'appuyer pour apprendre les bonnes pratiques et me guider dans la production des différents livrables inhérents à la réalisation d'un SMSI.

La série ISO 27000

La série ISO 27000 comporte une pléthore de normes concernant la sécurité informatique :

- ISO 27000 : Ce document offre une vue d'ensemble sur ce que couvrira la série ISO 27000. La terminologie et les définitions y sont également présentes.
- ISO 27001 : C'est la norme principale, qui cadre la mise en place du SMSI, à savoir spécifie les exigences de celui-ci, explique comment le mettre en œuvre et l'améliorer continuellement. De plus, on y trouve l'annexe A sur laquelle je peux me reposer pour ce qui est des différents domaines à sécuriser, qu'ils relèvent des aspects organisationnels (par exemple une Politique de Sécurité de l'Information), techniques

(par exemple l'authentification) ou bien même physique (par exemple l'accès physique à un local).

- ISO 27002 : Cette norme ISO se base directement sur l'annexe A de l'ISO 27001, et propose différents contrôles pour chacun des domaines à englober dans le SMSI.
- ISO 27003 : Ce standard décrit le processus de conception du SMSI, en passant par l'obtention de l'approbation de la Direction, jusqu'à la mise en œuvre. De plus, ce standard est particulièrement adaptable à tous types d'organisation, de sorte que les plus petites puissent simplifier les différentes activités et de sorte que les plus grandes puissent comprendre qu'une gestion en couches (par exemple les couches stratégique, tactique et opérationnel de l'ITIL) serait plus appropriée.
- ISO 27004 : Ce guide est orienté sur la phase post implémentation du SMSI, il décrit l'importance de mesurer l'efficacité du SMSI, comment le faire, et comment interpréter les résultats des mesures.
- ISO 27005 : Cette norme décrit la pratique d'analyse des risques, c'est à dire comment les identifier, comment les décrire, comment évaluer leurs criticités et comment les prioriser dans l'application des mesures correctives.
- ISO 27006 & 27007 : Ces deux documents sont des guides pour réaliser des audits.

Il y a bien d'autres normes ISO 27000 mais qui se concentrent dans des sujets de la sécurité bien spécifique. Par exemple l'ISO 27034 qui est focus sur la sécurité des applications. Néanmoins, pour mener à bien ce projet, j'estime ne pas avoir besoin d'entrer trop dans les détails des aspects de la sécurité des différentes composantes du SI.

Les publications du NIST

Le NIST, pour National Institute of Standards and Technology, en français "Institut National des Normes et de la Technologie" est, au même titre que l'ISO, un organisme publiant des standards de bonnes pratiques. Le NIST cependant est un organisme du département du Commerce des États-Unis, contrairement à l'ISO qui n'est rattaché à aucun gouvernement. Bien que le NIST soit basé aux États-Unis, il collabore avec des experts du monde entier. Donc tout comme les standards ISO, il est juste de se référer à leurs publications en matière de standards et de bonnes pratiques.

La cadre de cybersécurité

Le document du NIST le plus connu concernant la mise en place d'un SMSI est le Cybersecurity Framework[1], en français cadre de cybersécurité. C'est un document qui donne les lignes directrices pour la gestion et la mitigation des différents risques informatique, en se reposant sur des directives bien définis.

[1] Lien pour consulter le cadre de cybersécurité : https://doi.org/10.6028/NIST.CSWP.04162018fr

Les publications spéciales

Le NIST publie des "publications spéciales" nommées "SP" pour "Special Publication", qui couplées au cadre de cybersécurité, offrent des méthodes pour l'évaluation et la gestion des risques qui aident à la mise en place d'un SMSI.

Parmi ces publications, on peut en trouver deux qui sont primordiales :

- La NIST SP 800-53r5[2], est une publication détaillant les contrôles de sécurité. C'est dans ce document qu'on peut découvrir une liste exhaustive des différentes solutions techniques et managériales pour prévenir et réduire les risques.
- La NIST SP 800-37r2[3], est un document offrant un cadre sur la gestion des risques. Ce document est bien plus détaillé et précis que le Cybersecurity Framework. Il parle notamment de l'aspect de responsabilité des parties prenantes, des prérequis en termes de document (schémas du SI notamment), de la supervision et de l'évaluation du SMSI.
- La NIST SP 800-171r2, est une publication qui comme la NIST SP 800-53 liste les contrôles à appliquer pour la gestion des risques.

💡 **À noter, le suffixe "rX" comme à la fin du nom de la publication NIST SP 800-171r2 sert à déterminer le numéro de révision (ou de version) du document.**

Il existe bien d'autres publications traitant de la sécurité de l'information, cependant celles-ci peuvent être simplement complémentaires ou bien plus spécifique sur un sujet en particulier.

Cependant, j'ai deux publications qui peuvent paraître identiques, à savoir la NIST SP 800-53 et la NIST SP 800-171. Bien qu'elles listent les différents contrôles à appliquer, la NIST 800-53 est particulièrement exhaustive et bien plus lourde à appliquer pour un organisme n'ayant pas besoin de traiter des informations classifiées secret défense. En revanche, la NIST SP 800-171 se concentre sur les contrôles à appliquer dans le cadre de traitement d'informations comme des données personnelles.

La NIST SP 800-171 sera donc plus applicables et cohérentes dans le cadre de la mise en place du SMSI dans l'organisme de formation PHILIANCE.

Résumé

J'ai donc à disposition deux types de publication de deux organisations différentes. L'organisation ISO qui publie des standards payants, mais pour lesquels j'ai accès grâce à la bibliothèque ENI. Et l'organisation NIST qui publie des standards publics.

[2] NIST SP 800-53r5: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[3] NIST SP 800-37r2: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Peu importe la publication de ces deux organisations, je suis certain que celles-ci pourront me guider dans la création d'un SMSI dans les règles de l'art.

Enfin, pour répondre à ma problématique d'intégration d'un SMSI dans une TPE/PME, je pourrais adapter les méthodologies et les pratiques pour les rendre adéquates aux besoins de PHILIANCE.

Deuxième partie : L'état de la sécurité informatique en Europe et en France

Rapport de l'ENISA

L'ENISA, European Union Agency for Cybersecurity, en français "Agence de l'Union Européenne pour la Cybersécurité", a publié un rapport annuel concernant l'état des cyberattaques au niveau Européen. Depuis ce rapport je peux me faire une idée globale de la cybersécurité, et de l'importance du projet d'intégration du SMSI.

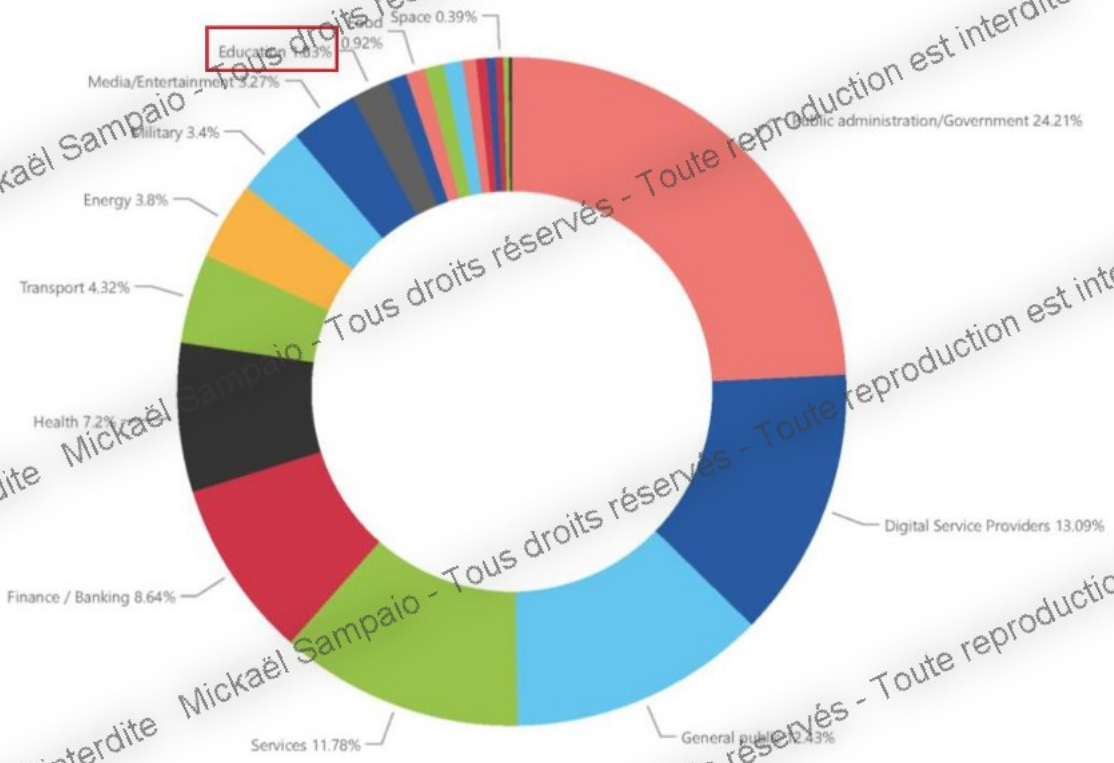
Le rapport que je vais présenter est publique et sa reproduction est autorisée conformément aux droits d'auteurs explicités sur le site de l'ENISA et accessibles via ce lien : https://www.enisa.europa.eu/about-enisa/legal-notice

Ce rapport[4], communément appelé ETL pour "Enisa Threat Landscape" a été publié en Novembre 2022.

Le schéma ci-dessous représente la répartition des incidents de sécurité en pourcentage par domaine d'activité :

[4] Rapport ENISA Threat Landscape 2022, téléchargeable via le lien : https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Figure 4: Targeted sectors per number of incidents (July 2021-June 2022)



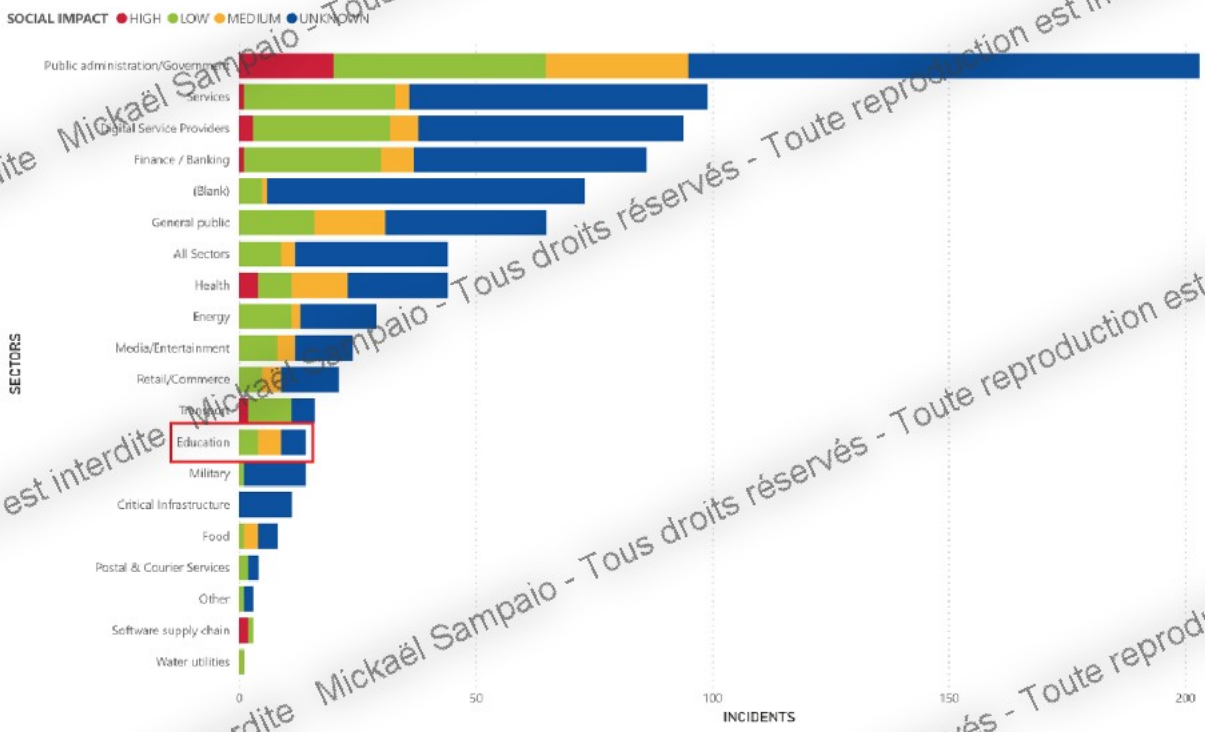
Je constate que le secteur de l'éducation est touché par 1.83% des cyberattaques totales sur l'année 2021-2022.

💡 **Une statistique représentée sur le site statista.com affiche le secteur de l'éducation comme touché par 7.3% des cyberattaques[5]. Statista.com est réputé fiable car les statistiques générées se bases sur diverses sources fiables. Cependant cette statistique regroupe des sources mondiales et non Européennes, d'où la différence notable.**

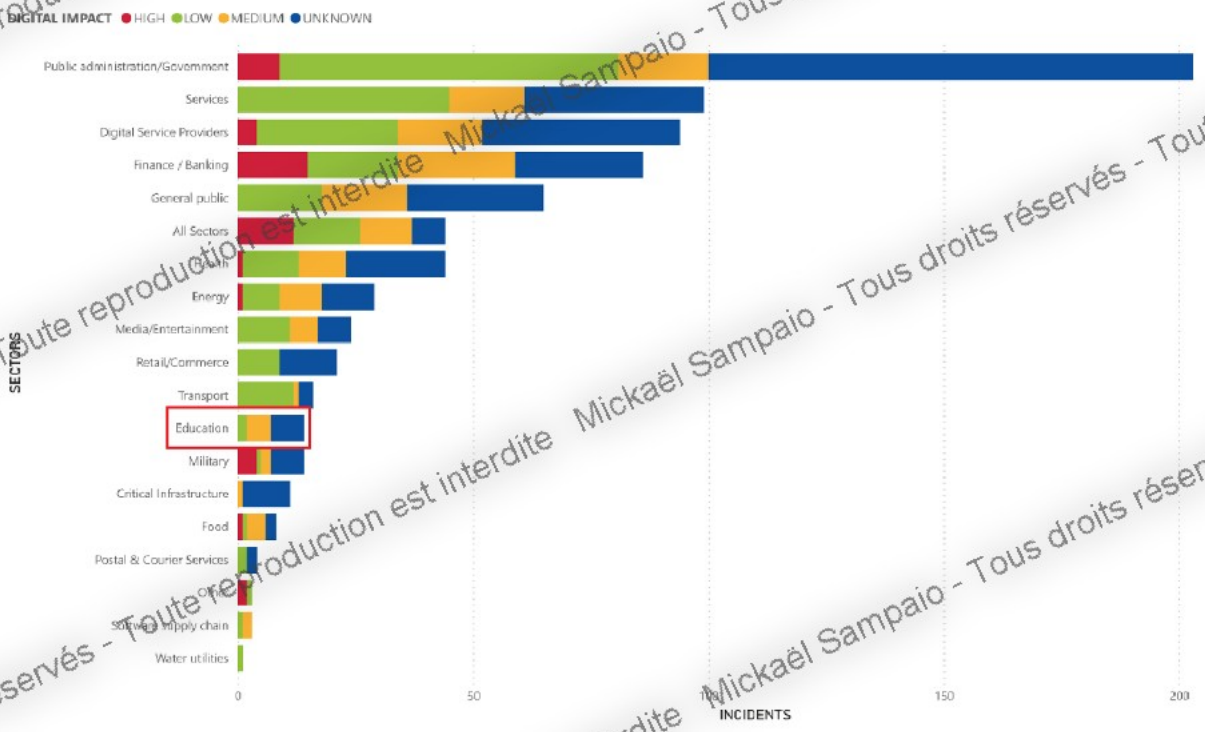
[5] Distribution des cyberattaques à travers les industries mondiales en 2022, Statista.com, lien : https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

Sur les deux schémas ci-dessous, je peux voir les domaines les plus impactés par une cyberattaque dans le secteur de l'éducation :

Impact sociétal :



Impact digital :

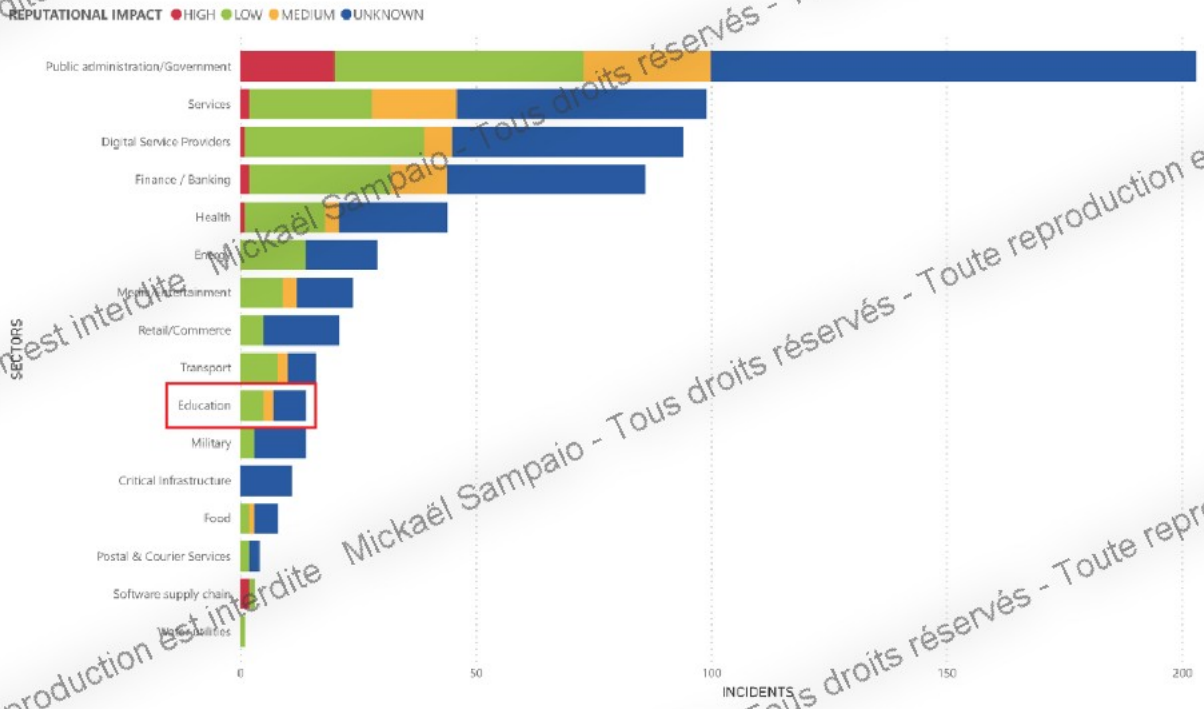


L'impact sociétal se réfère à l'impact sur les services publics et sur la société en général, et l'impact digital se réfère à l'impact sur le système d'information et les données en général.

On peut voir sur ces schémas que le secteur de l'éducation a un impact MEDIUM, en français "moyen", représenté en jaune, sur l'impact social et sur approximativement 30% des incidents. Concernant l'impact digital, l'impact moyen est estimé sur approximativement 25% des incidents.

Il y a également d'autres domaines impactés mais plus faiblement.

Cependant, j'estime qu'il est important de se référer également à l'impact sur la réputation comme le montre le schéma ci-dessous :



L'impact sur la réputation, qui se réfère à la perte de confiance publique et des clients, est estimé globalement assez faible. L'impact moyen est estimé approximativement sur 15% des incidents totaux.

Néanmoins, PHILIANCE est un organisme qui forme principalement dans le domaine du numérique, et j'estime que l'impact sur la réputation de PHILIANCE serait bien plus fort qu'un autre organisme de formation orienté sur des spécialités autres que le numérique.

J'ai donc des statistiques fiables concernant la répartition des cyberattaques par secteur, et les domaines les plus impactés lors d'une cyberattaque dans le secteur de l'éducation.

Cependant, cela ne reste que des pourcentages, et pour avoir des statistiques cohérentes, il faut des nombres qui couplés aux pourcentages permettent de se représenter vraiment l'état global des cyberattaques.

Parmi ces nombres, j'ai besoin du nombre d'attaque, et du coût moyen d'une cyberattaque.

Statistiques d'Asterès

Asterès est un cabinet d'études, de recherche et de conseil économique réputé. Ce cabinet a été mandaté par le CRiP, Club des Responsables Infrastructures, Technologies et Production IT, pour effectuer des recherches sur le coût des cyberattaques réussies en France.

D'après l'étude menée[6] :

- Le coût total lié aux cyberattaques en France est de 2 milliards d'euros en 2022.
- Ce coût comprend : des coûts directement liés à l'attaque (mobilisation des équipes internes et externes, sollicitation d'avocats) de 887 milliards d'euros, des coûts des rançons à 888 milliards d'euros et des coûts de perte de production de 252 millions d'euros
- En moyenne, 1,8 cyberattaque réussie par organisation et par an pour un total de 385 000 cyberattaques réussies en 2022
- Le coût moyen d'une cyberattaque de type ransomware est de 59 000 euros.
- Le coût moyen d'une cyberattaque non ransomware est de 33 300 euros.

[6] Les cyberattaques réussies en France : un coût de 2 Mds€ en 2022, Asterès, lien : https://asteres.fr/site/wp-content/uploads/2023/06/ASTERES-CRIP-Cout-des-cyberattaques-reussies-16062023.pdf

De plus, un tableau représentant approximativement les ordres de grandeur du volume de cyberattaque en France par type d'organisation a été modélisé :

Tableau 1. Calcul du volume de cyberattaques en France, par type d'organisation

	Nombre total d'organisations	Dont victimes de cyberattaque (s)	Nombre total de cyberattaques en 2022
Entreprises (hors microentreprises)	154 189	80 800	347 441
Dont PME	148078	76 852	330 466
Dont ETI	5841	3 773	16 225
Dont GE	270	174	750
Collectivités territoriales/locales	18 052	5 096	21 911
Dont régions	18	8	35
Dont départements	101	45	195
Dont communes > 10 000 hab.	1 018	458	1 970
Dont communes de 500 à 9 999 hab.	16 915	4 584	19 711
Établissements de santé	2989	1 744	7 498
Dont public	1347	683	2 937
Dont privé	1642	1 061	4 561
Établissements d'enseignement supérieur	3500	1 775	7 630
Autres établissements publics	122	62	266
Dont EPIC	51	23	99
Dont EPA	71	32	137
Ministères	15	8	33
Total	178 867	89 483	384 779

Je constate avec ce tableau qu'en 2022, environ une PME sur deux a été victime d'une cyberattaque.

Informations diverses

D'après le pôle cyber du gouvernement Français[7], les petites entreprises TPE/PME sont plus susceptibles d'être visées par des cyberattaques. En effet, celles-ci sont moins consciente des risques inhérents à l'informatique, et elles pensent, à tort, que leurs activités ou leurs tailles ne sont pas intéressantes pour les cybercriminels.

Cependant c'est l'inverse qui est constaté. Les TPE/PME ne sont pas ou peu protégées contre les risques cyber et n'incluent pas la gestion de la sécurité de l'information dans leurs organismes, ce qui fait une d'eux une cible de choix pour les cybercriminels.

À cela s'ajoute que les TPE/PME sont souvent fragiles financièrement et une cyberattaque peut rapidement mener à la faillite de l'entreprise.

[7] La cybersécurité pour les TPE/PME – enjeux et solutions, cybermalveillance.gouv.fr, lien : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-tpe-pme-enjeux-solutions

D'après Almeria, une entreprise fournisseur de solution informatique, 60% de TPE/PME cessent leurs activités dans les 6 mois suivant une cyberattaque[8]. Le coût que représente une cyberattaque pour une PME française est de 10 000 euros à 100 000 euros, la moyenne rejoignant celle annoncé par l'étude d'Asterès.

D'après une étude de Kaspersky, une entreprise de solution de cybersécurité, 90% des brèches de cybersécurités sont causées par une erreur humaine[9].

Résumé

J'ai appris que le secteur de l'éducation est loin d'être le plus visé par les cybercriminels. Cependant, j'ai découvert que les TPE/PME sont plus ciblées que des entreprises de plus grande envergure.

Je sais qu'un organisme français qui subit une cyberattaque de type ransomware subit une perte moyenne de 59 000 euros. Une attaque qui ne demande pas de rançon peut s'estimer à 33 300 euros. De plus, j'ai appris qu'il y a des coûts indirects à une cyberattaques, tel que la perte de réputation qui sur long terme peut avoir un impact notable.

Je sais qu'une TPE/PME a de forte chance de cesser ses activités à la suite d'une cyberattaque si celle-ci y est mal préparée.

Enfin, 90% des cyberattaques réussies proviennent d'une cause humaine, et donc du manque de sensibilisation et de formation sur les risques cyber.

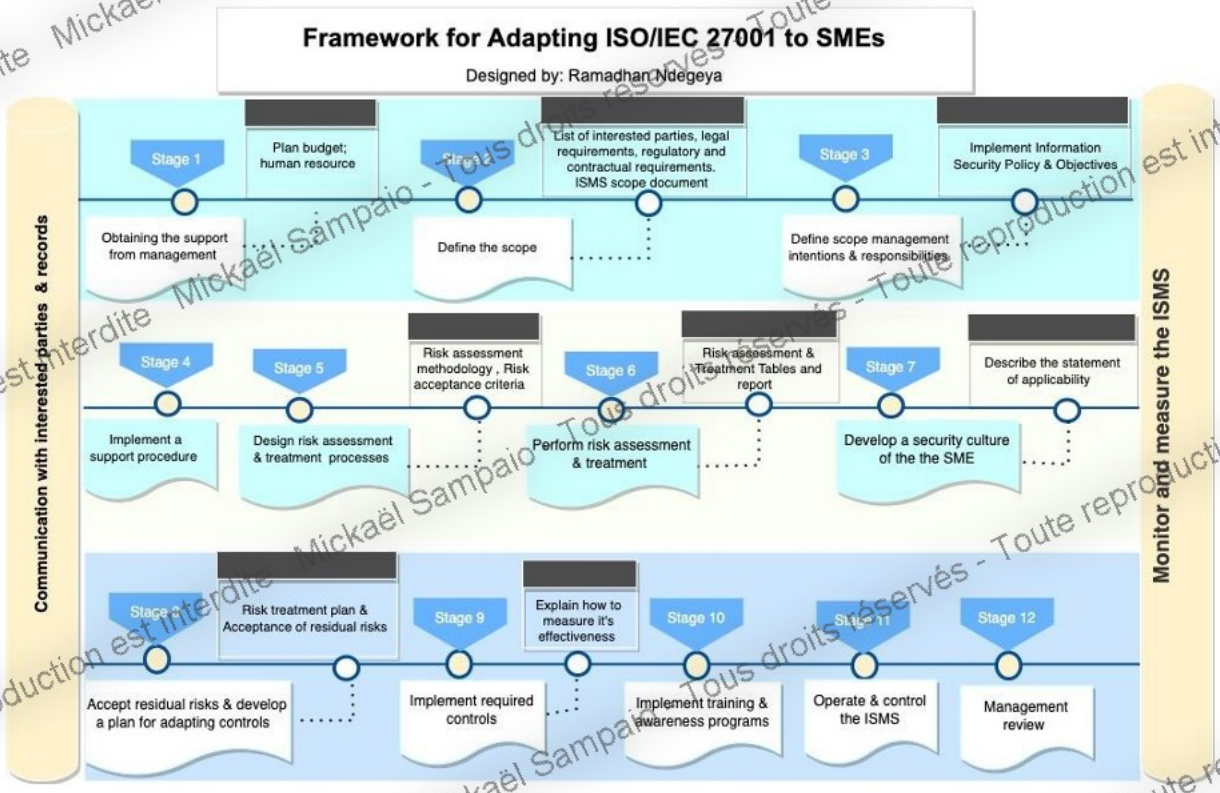
[8] Les cyberattaques se sont multipliées en 2020, Almeria, lien : https://www.almeria.fr/2020/12/04/les-cyberattaques-se-sont-multipliees-en-2020/

[9] Le facteur humain est un enjeu majeur de la cybersécurité en entreprise, Kaspersky, lien : https://media.kaspersky.com/fr/business-security/enterprise/Fiche-Kaspersky-Security-Awareness_Facteur-humain.pdf

Troisième partie : Adapter le SMSI pour une TPE/PME

Le cadre pour adapter le SMSI aux TPE/PME de Ramadhan NDEGEYA

Sur LinkedIn, j'ai découvert un cadre pour mettre en place et adapter le SMSI au TPE/PME, créé par Ramadhan NDEGEYA, expert en cybersécurité[10].



Ramadhan définit les différentes étapes ainsi :

- Obtenir le soutien de la Direction : C'est la Direction qui valide tout projet et tout investissement. Il est donc évident de devoir commencer par avoir le soutien de celle-ci. De plus, il faut obtenir une forte implication de la Direction dans le projet pour avoir son appui dans les étapes suivantes telles que la définition des responsabilités, la communication en interne mais également en externe (partenaires, fournisseurs, prestataires).
- Définir le périmètre : C'est l'étape où on va définir ce qui est à intégrer dans le projet et ce qui est à exclure. La plupart des entreprises préfères se concentrer sur les actifs sur site et tendent à ne pas inclure les actifs hors site. Cependant, l'ISO 27001 exige que tous les actifs traités par l'organisme doivent être pris en compte. Les cas d'exclusion et de priorisation seront à définir dans cette étape. On définira également

[10] Cadre pour adapter l'ISO/IEC 27001 aux TPE/PME, Ramadhan NDEGEYA, lien : https://www.linkedin.com/pulse/how-implement-iso27001-smes-ramadhan-ndegeya/

les responsabilités des parties prenantes, les réglementations, les politiques de sécurité et les objectifs.

- Rédiger la politique de sécurité du SMSI : Si un des objectifs du projet est de passer la certification ISO, alors il est nécessaire de rédiger une politique de sécurité pour expliquer la stratégie de sécurité de l'entreprise, pour stipuler les objectifs à atteindre et les contrôles s'y afférent.
- Concevoir le processus d'évaluation et de traitement des risques : C'est dans cette phase qu'on va définir comment les risques seront identifiés et gérés, et qu'on définira l'impact et la probabilité de chaque risque.
- Effectuer l'évaluation des risques : C'est un processus continue qui vise à évaluer les différents risques, et les prioriser. Pour ce faire on se base sur le processus défini précédemment. C'est après cette évaluations des risques qu'il sera plus clair de définir les contrôles à appliquer.
- Mettre en œuvre les contrôles requis : Dans cette étape, on s'occupe d'appliquer les contrôles pour mitiger les risques évalués en amont. Par contrôle on parle de procédures, de documentation, et de solutions techniques. Ramadhan appuie également sur le fait qu'il ne faut pas ignorer des procédures définies, ce que font la plupart des TPE/PME.
- Mettre en œuvre des programmes de formation et de sensibilisation : Une phase cruciale, la formation et la sensibilisation aux risques. Car même si les politiques de sécurité sont bien formalisées, que les mesures techniques sont parfaites, il reste primordial de former les employés. Il faut faire une formation au minimum deux fois par an, ce que la plupart des PME ne font pas.
- Opérer le SMSI : Cela signifie que l'entreprise doit adopter la gestion du SMSI comme une routine quotidienne, où on va surveiller le bon fonctionnement des contrôles mis en œuvre, réviser les documentations et récolter les journaux continuellement.
- Faire examiner le SMSI par la Direction : Il est important que la Direction ai connaissance de tous les rapports, actions et audits effectués au sein du SMSI.
- Surveiller et mesurer le SMSI : C'est une phase où les TPE/PME ont du mal à être rigoureuse. Pourtant, c'est cette étape continue qui fournit des résultats clairs sur ce qu'il se passe au sein du SMSI, à savoir les incidents qui sont apparus, comment ils ont été résolus, et la situation actuelle. De plus j'ajoute que c'est à partir de cette étape qui est continue qu'on pourra appliquer une réelle amélioration continue du SMSI.

La publication de Nicolas MAYER

Nicolas MAYER, chercheur dans le domaine des sciences et de la technologie, a publié un guide[11] conjointement avec Thierry VALDEVIT et Béatrix BARAFORT, pour implémenter un SMSI dans une petite structure.

D'après les recherches menées sur une entreprise cobaye, Codasystem, les trois chercheurs ont définis six objectifs pour adapter le SMSI aux TPE/PME :

- Objectif 1 : Revoir à la baisse les exigences de l'ISO/IEC 27001 pour rendre les rendre plus accessibles aux TPE/PME qui ont des ressources limitées
- Objectif 2 : Affiner l'approche de sécurité pour les utilisateurs, et éviter que le SMSI soit perçue comme une contrainte mais plutôt comme un bénéfice.
- Objectif 3 : Donner les recommandations majeures et génériques, qui sont à détailler pour expliquer comment ces actions affecteront le système dans son entièreté.
- Objectif 4 : Prévoir un guide d'implémentation pour chaque processus du cycle PDCA. Contrairement à l'ISO/IEC 27001 qui présente les exigences de manière approximative, il faudra simplifier au maximum les exigences dans un modèle clair.
- Objectif 5 : Assurer la cohérence et la fiabilité du guide qui est à définir. Il faut garder à l'esprit qu'il faut suivre les recommandations de l'ISO/IEC 27001 et être aligné avec ses exigences.
- Objectif 6 : Offrir des outils pertinents. Il faut définir des modèles de documents, et des outils pour les rédiger afin d'accélérer au possible le processus de documentation.

Résumé

J'ai donc une confirmation que la Direction doit être sincèrement engagée et impliquée dans le projet.

De plus, j'ai un schéma visuel qui me permet d'avoir une chronologie des étapes à respecter et adaptée à l'intégration d'un SMSI dans une TPE/PME.

Je peux et je vais devoir modifier certains des modèles de documents donnés dans les standards ISO, pour les rendre moins lourds et plus compréhensibles.

Je vais devoir bien expliquer l'intérêt du projet du point de vue de chacun des parties prenantes pour éviter au maximum que le projet soit vu comme une contrainte mais comme un bénéfice.

Malgré les libertés que je peux prendre, je dois respecter les exigences des standards ISO.

[11] Adapter l'ISO/IEC pour les PME : Un guide pour mettre en place un SMSI dans des petites structures, de Thierry VALDEVIT, Nicolas MAYER, et Béatrix BARAFORT, lien : https://nmayer.eu/publis/EuroSPI2009-Valdevit_Mayer_Barafort.pdf

Je vais devoir expliquer l'intérêt et les objectifs de chaque cycle du PDCA dans le cadre du projet.

Pour finir, je dois trouver un moyen simple de transmettre les informations à la Direction, si possible l'automatiser, pour éviter l'omission de l'étape continue de surveillance et de mesure du SMSI.

Cadrage du projet

Ressources du projet

Ressources humaines

Pour mener à bien ce projet, j'ai besoin de définir les différents acteurs et parties prenantes, mais également chacun des collaborateurs.

En premier lieu, je suis l'acteur principal et responsable du projet. C'est moi qui définirai chaque brique du projet, qui récoltera et centralisera les informations, qui rédigera chacun des livrables nécessaires et qui proposera les méthodologies pour mener à bien la définition du SMSI.

Mon tuteur sera la première personne qui validera chacun des éléments du projet si besoin, avant de les soumettre pour une seconde validation par la Direction.

Je solliciterai également le service informatique à savoir Julien DAVROUX, Julio NDONG, et Florian VERON pour chaque élément qui nécessitent d'avoir une totale objectivité, on peut par exemple penser à la cartographie des risques.

Les choix de solutions techniques pour répondre aux différents besoins qui seront explicités par le SMSI seront définis par Julio NDONG, administrateur système et réseau.

La Direction devra valider ou demander des révisions sur tous les livrables proposés. C'est uniquement après validation de chacun des livrables et donc du SMSI dans sa finalité, que celui-ci sera approuvé définitivement.

Enfin, les tous les collaborateurs seront sollicités. En effet, dans le cadre de la cartographie des processus, j'aurai besoin de comprendre en détail chaque activité de tous services confondus.

Pour mieux se représenter les différents acteurs, j'ai réalisé une matrice RACI. Une matrice RACI permet de représenter sous une forme matricielle les rôles de chaque acteur, direct ou indirect d'un projet, où :

- (R) Responsible : est une personne qui va exécuter la tâche et qui en est responsable
- (A) Accountable : est une personne qui va approuver la tâche et qui en a l'autorité
- (C) Consulted : est une personne qui va être consulté dans l'exécution de la tâche
- (I) Informed : est une personne qui sera informée lorsque la tâche sera finie

De plus, j'ajoute que définir une matrice RACI est importante non seulement pour bien définir les rôles, mais également pour calibrer pertinemment l'intérêt pratique des rôles de chacun. Inclure trop d'acteur dans la réalisation d'une tâche peut impacter sérieusement le temps qu'une tâche peut prendre, et ce surtout si les avis sont contradictoires dans la façon de réaliser la dites tâche.

J'ai donc réalisé cette matrice RACI :

	Mickaël SAMPAIO, Apprenti Cybersécurité	Julien DAVROUX, DSI	Julio NDONG, Administrateur Système et Réseau	Florian VERON, Assistant Technique	Collaborateurs	Direction
Communication aux collaborateurs	R	C	I	I	I	A
Cartographie des processus	R	A / C			C	C
Schéma de flux réseau	R	A	I	I		
Classification des données	R	A / C	C	C	I	I
Cartographie des risques	R	A / C	C	C	I	I
PSSI	R	A	I	I	I	C
Plan de gestion des incidents	R	A	I	I		I
Modèle de document de rapport mensuel	R	A	I	I		C

Définition du cycle PDCA	R	A	C			I
Choix des solutions techniques	C	A	R			I
PCA / PRA	R	A	C			I
Déclaration d'applicabilité	R	A	C			I
Plan de formation et de sensibilisation	R	A	I	I	I	C
Rapport de projet	R	A	I	I	I	I

Budget

Pour ce qui est du budget d'un tel projet, il n'y aucun coût matériel ou logiciel à inclure, car le SMSI est un ensemble de documents, de procédures et de politiques. Néanmoins, en aval du projet, il faudra bien évidemment respecter les besoins explicités du SMSI, et c'est le budget de ceux-ci qui incluront probablement divers achats, notamment des logiciels de sécurité ou du matériel comme un pare-feu par exemple.

Cependant, la rédaction de tous les livrables nécessaires au SMSI représente un coût humain conséquent par la complexité et le temps que cela prend.

Je vais me baser sur la création de la cartographie des processus pour expliquer comment je peux la budgétiser :

Je suis apprenti en cybersécurité et je suis responsable de la définition de la cartographie des processus. Je n'ai jamais réalisé de cartographie des processus, et je dois effectuer des recherches sur les standards, normes, retour sur expérience, pour créer une cartographie cohérente et surtout intuitive. J'estime une matinée de recherche pour combler ce manque de connaissance, soit trois heures et demie. Avec trois ans d'ancienneté j'ai une bonne connaissance du fonctionnement organisationnel et opérationnel de l'entreprise, mais je vais devoir m'en assurer, et combler mes manques s'il y en a. Je vais donc devoir échanger avec chacun des responsables de services.

Il y a plusieurs responsables de services :

- Émilie TESSIER, Directrice Générale
- Charlotte TESSIER, Responsable RH
- Fabien ZIND, Responsable Services Généraux
- Julien DAVROUX, Directeur du Système d'Information
- Aïssata NDIAYE, Responsable Pédagogique des cursus
- Steny ARCHINART, Responsable Administrative des cursus
- Christophe ZIND, Responsable de la formation continue
- Jalila TABYAK, Responsable du service Retour à l'Emploi
- Vanessa MANFREDI, Responsable Marketing & Commercial
- Zakaria SAOUDI, Responsable Finance
- Mithula KANDIAH, Responsable Ingénierie Pédagogique

Je vais devoir demander du temps à chacun des responsables listés ci-dessus, en moyenne je peux estimer une matinée entière d'échange pour avoir une analyse profonde de leurs activités et des processus inhérents à leurs services respectifs et aux échanges interservices.

Il est à noter que les processus ne sont pas tous correctement définis et cadrés, et qu'il sera également de m'on ressort, avec la collaboration de la Direction de rectifier certain processus pour les rendre plus cohérent, et moins chronophage si possible. Sachant qu'il y a environ en moyenne 50% des activités quotidiennes de chacun des collaborateurs qui ne sont pas clairement définis et chacun travail un peu comme il peut pour atteindre des objectifs qui eux sont bien définis.

J'ai donc onze personnes avec qui je dois échanger, avec une matinée, soit trois heures et demie à peu près, à réserver par personne. À cela s'ajoute une multiplication de 50% du temps avec chacun des responsables pour les rectifications des processus.

Une réunion doit être préparée et un ordre du jour clairement défini pour éviter au maximum les écarts pendant les échanges. J'estime cette préparation d'environ 30 minutes que je multiplie donc par onze, le nombre de responsable.

Pour simplifier les calculs et parce-que je n'ai pas connaissance de la rémunération de chacun, je vais me baser sur un taux horaire au SMIC de mai 2023 qui est de 11.52€ brut.

J'ai donc : 11 responsables qui vont être missionnés pendant 3h30 chacun soit 11x3.5 = 38.5 heures que je multiplie par 2 car je serais évidemment moi-même missionné soit 38.5x2 = 77 heures. Je multiplie par 50% pour les rectifications des écarts dans les processus soit 77x1.5 = 115.5 heures. J'additionne 115 heures et demie de réunions avec les 11 préparations de réunion donc 115.5 + 11x0.5 = 121 heures.

121 heures de temps de travail sur un taux horaire brut de 11.52€ est égale à 1393.92€

Le calcul final est de **1393.92€** de coût humain uniquement pour la première partie de la cartographie des processus, qui est l'analyse de l'existant

La seconde partie étant la création de la cartographie des processus avec les résultats de la première partie.

Je n'ai pas besoin de solution logiciel payant, je peux me baser sur des outils gratuits.

J'estime la création de la cartographie complète de PHILIANCE en à peu près quatre jours.

On a donc quatre jours de travail, je travaille 7 heures par jours soit 7x4x11.52€ = 322.56€

La dernière partie est la phase où il y a une revue finale et des ajustements si nécessaire :

Je vais devoir de nouveau consulter les onze responsables de service et j'estime une heure d'échange avec chacun

Je pense avoir 30% de la cartographie à revoir

J'ai donc 11 heures d'échanges avec les responsables auquel je m'ajoute, soit 22 heures et je refais 30% de la cartographie qui m'avait initialement pris 28 heures, je fais donc le calcul avec le taux horaire (22+28x0.3)x11.52 = 352.21€

Le coût total estimé est donc de 1393.92€ + 322.56€ + 352.21€ soit 2068.69€

Pour tout projet où un coût est estimé, je rajoute également une marge de 20% pour anticiper les écarts. Le coût estimé revient donc à 2068.69x1.20 = **2482.43€**

Il est à noter que ceci reste une sérieuse approximation, car j'aurai pu aller plus loin dans le calcul pour être plus proche de la réalité. En effet, j'ai intentionnellement omis certains facteurs ou actions tels que :

- La communication en amont pour rassurer les collaborateurs et les faire adhérer à la conduite du changement
- Les coûts indirects :
    - Coûts électriques, qui s'additionne à chaque activité où poste de travail, télévision ou autre est utilisé
    - Coûts des locaux
    - Le travail à effectuer pour convaincre la Direction du financement du projet

💡 **À noter que pour être plus juste sur les calculs de budgétisation, je pense qu'il serait intéressant d'estimer le coût horaire d'un salarié en incluant les coûts indirects qui sont présent en tout temps, tel que l'électricité par exemple, qui est constamment utilisée, chacun des collaborateurs utilisant un poste de travail pour son activité professionnelle.**

Périmètre du projet

Objectifs

Différents objectifs sont attendus pour l'intégration d'un SMSI au sein de PHILIANCE.

Premièrement, un objectif de sécurité de l'information, c'est l'intérêt principale d'un SMSI, et c'est sur la réponse au besoin de sécurité que je vais baser chacun des livrables attendus.

On attend de ce projet de mitiger tous les risques connus, et d'anticiper un maximum les risques inconnus.

Par risques connus je fais référence à des risques qui ont été identifiés et documentés, par une expérience passée ou bien connus grâce à des sources externes par la veille technologique notamment.

Par risques inconnus, je fais référence aux risques qui peuvent ne pas être entièrement pris en compte dans les solutions techniques et méthodologies de réponse aux incidents, car ce sont risques qui proviennent de facteurs imprévus et pour lesquels aucune gestion spécifique n'est prévue.

Ce projet étant focus sur la sécurité, je lui trouve également d'autres intérêts significatifs :

- Un gain de production par la création de la cartographie des processus.
- La mise en conformité réglementaire en respectant les différentes lois.
- La possibilité de passer des certifications ISO ou d'être agréer en tant qu'organisme respectant des mesures de sécurité cadrées. Ce qui amène à une confiance accrue des clients et un gain certain de compétitivité.
- L'adoption de bonnes pratiques dans le cadre de la sécurité de l'information peut également mener à d'autres projets de mise en place de bonnes pratiques dans d'autres aspects de l'organisation. C'est à dire d'adopter une démarche de qualité.
- L'établissement d'un cadre juridique clair et précis sur lequel PHILIANCE peut se baser dans le cadre où un interne ou un partenaire venait à ne pas respecter ses obligations qui sont définis dans les politiques de sécurités. (Exemple : vol de données, sabotage)

Parties prenantes

Il est important de définir les parties prenantes en amont du projet pour cadrer celui-ci et avoir d'emblée une vision d'ensemble du projet. De plus, cela permet d'éviter l'omission de certains pendant le projet.

Je liste donc les différentes parties prenantes :

- Les internes, ce sont les collaborateurs de PHILIANCE :

- Émilie TESSIER, Directrice Générale, qui sera une actrice importante dans le projet car c'est elle qui validera définitivement les livrables.
- Charlotte TESSIER, Responsable Administrative interne et Ressources Humaines, qui traite d'informations sensibles et qui risque d'être fortement impactée par les changements
- Gaëlle TESSIER, Responsable Pôle Sanitaire et Social
- Julien DAVROUX, Directeur du Système d'Information, qui sera missionné et consulté pour certaines tâches et qui validera certains livrables avant l'approbation final de la Direction
- Fabien ZIND, Responsable Services Généraux
- Christophe ZIND, Responsable Formation Continue
- Jalila TABYAK, Responsable Commercial et Retour à l'Emploi
- Allan DAUVERGNE, Coach Emploi
- Cloé DELZENNE, Responsable Formation Alternance
- Aurélia BATU, Chargée d'Admission
- Steny ARCHINART, Responsable Administrative des cursus, qui traite massivement des données personnelles des apprenants et qui risque d'être fortement impactée par les changements
- Aïssata NDIAYE, Responsable Pédagogique des cursus
- Alioune NDOYE, Apprenti Commercial
- Sofiane KRIKABE, Apprenti Commercial
- Mithula KANDIAH, Responsable Ingénierie Pédagogique
- Stéphanie DEVAUX, Référente Pédagogique
- Clément HURMAN, Responsable Test de Connaissance du Français
- Zakaria SAOUDI, Responsable Finance
- Vanessa MANFREDI, Responsable Marketing & Commercial
- Barbara TOROSSIAN, Standardiste
- Florian VERON, Assistant Technique, qui sera consulté pour certaines tâches
- Julio NDONG, Administrateur Système et Réseau, qui sera missionné et consulté pour certaines tâches.

- EUREKA, c'est le groupement auquel PHILIANCE appartient, je pense qu'il serait intéressant que la Direction d'EUREKA soit au courant du projet d'intégration de SMSI pour renforcer leur confiance envers PHILIANCE. De plus, EUREKA bénéficie peut-être également de ressources qui pourrait être utile à ce projet, comme des experts juridiques, des responsables de la sécurité du système d'information, ou bien des exemples de cartographies de processus.
- DORANCO, c'est un organisme de formation partenaire, faisant également parti du groupe EUREKA. C'est le principal organisme certificateur.

- Pôle Emploi, un organisme des services publics qui redirige un nombre conséquent de demandeur d'emploi dans nos cursus de formations. Il est à bien prendre en compte que nous recevons donc d'eux une masse importante de données personnelles et sensibles.
- Xonatis, c'est un groupe de développement web, qui est notamment en cours de développement d'Educentre, une plateforme pour gérer des cursus de formation, que PHILIANCE utilise.

Exclusions

Il est important de correctement définir ce qui est exclu du périmètre du projet, pour maximiser le focus du projet sur les éléments les plus importants, éviter les risques de trop s'éparpiller sur des points inutiles et donc de réduire la valeur du projet.

J'écarte donc du projet les locaux du Parc Élysée et de Créteil car il est fort probable que PHILIANCE se sépare de ceux-ci prochainement.

Contraintes

Ce projet a été validé en milieu d'année 2023 et j'ai eu une contrainte de temps très importante car je fini mon apprentissage en octobre 2023. Or ce projet est extrêmement complexe et nécessite un investissement conséquent en temps et il est certain que je ne pourrai pas le mener à terme en quelques mois. Cependant, Florian VERON qui occupe le poste d'assistant technique va intégrer une formation d'Administrateur Cybersécurité et Cloud en alternance, et il est prévu qu'il reprenne la continuité du projet dès mon départ. Je vais donc devoir poser des bases saines pour lui laisser un cadre bien défini sur lequel il pourra se reposer pendant la poursuite du projet.

Enfin, selon ce que pourrais produire pendant le temps qu'il me reste, je pense qu'il serait intéressant d'établir partiellement le SMSI en me focalisant sur un des quatre domaines de l'annexe A de l'ISO 27001:2022 à savoir, le personnel, l'organisation, la technique, ou l'accès physique.

Dépendances

Il y a en parallèle de ce projet de SMSI, un projet futur de restructuration du système informatique dans sa globalité. C'est Julio NDONG, administrateur système & réseau, qui en aura la responsabilité. Cependant bien que certain que ce projet se concrétise, il n'est pas enclenché. Je n'ai donc aucune planification de celui-ci, aucun plan d'architecture technique, ni même une vague idée de quand ce projet démarrera.

La seule directrice dont j'ai connaissance, c'est qu'un déploiement massif sur la solution cloud Microsoft 365 est prévue en premier lieu. Le but étant de proposer aux collaborateurs un environnement collaboratif répondant à quasiment tous les besoins de chaque service.

À la suite du déploiement de Microsoft 365, une refonte totale du système informatique sur site sera faite, à savoir, la mise en place de serveur Windows, la création d'un domaine et un déploiement de différents rôles et fonctionnalités pour la gestion interne du parc informatique. À cela s'ajoutera très probablement du matériel ou des services destinés à la virtualisation, la sécurité (pare-feu, IDS/IPS, EDR), ou bien à la supervision. Et c'est précisément cette partie qui a été à peine évoquée bien que sûr que cette mise en place arrivera prochainement.

Et justement, mon projet de SMSI apportera un contexte notable de sécurité quant à la définition du projet de restructuration du SI.

Néanmoins, avoir un plan d'architecture technique définit m'aurait particulièrement aidé pour l'identification des risques, la définition des PCA et PRA, et pour bien d'autres livrables.

Il me faudra garder cela en tête pour adapter la priorisation des mesures de traitement des risques et éviter par exemple de définir la mise en sécurité du partage Samba sous Linux comme de haute priorité alors que celui-ci est voué à disparaître prochainement.

Livrables

Il faut dès le départ lister l'intégralité des livrables, surtout pour un tel projet, un SMSI étant composé essentiellement de documents. Cela permet de plus facilement décomposer les différentes phases du projet et d'éviter des oublis.

Les livrables attendus pendant ce projet sont :

- La cartographie des processus : élément qui me permettra d'avoir une meilleure vision sur les ressources à l'entrée et à la sortie d'un processus pour aider à une meilleure identification des risques.
- Schéma réseau : comprendre l'ensemble du ou des réseaux et de chaque flux me permettra d'avoir une vue d'ensemble de celui-ci pour analyser les SPOF, anticiper les goulots d'étranglements, et mieux définir les solutions techniques à proposer pour répondre aux besoins en termes de réseautique de manière générale.
- Classification des données : c'est un des livrables les plus importants, en effet, c'est avec celui-ci que je vais pouvoir estimer les données les plus importantes à prioriser dans le cadre de la mise en application de la sécurité selon les critères de DICT.
- Cartographies des risques : j'estime que c'est le livrable clé du projet, la cartographie des risques initiales va me permettre d'avoir une vision claire des bénéfices apportés par chacun des autres livrables. En effet, quasiment tous les livrables sont censés réduire la criticité de chacun des risques identifiés.
- PCA / PRA : ces documents permettent de s'assurer que le SI reste fonctionnel en tout temps, et donc que la production reste continue même en temps de crise.

- PSSI : ce sont les diverses politiques de sécurité qui poseront un cadre réglementaire sur les multiples aspects de la sécurité de l'information.
- Plan de gestion des incidents : ce document sera une trame, une méthode à suivre dans le cas d'un incident, pour mener au rétablissement normal du SI et assurer la bonne communication aux différents acteurs impactés et à la Direction.
- Déclaration d'applicabilité : ce document centralisera les différentes mesures adoptées pour répondre aux exigences de sécurité de l'ISO 27001, il est obligatoire si PHILIANCE souhaite passer la certification.
- Modèle de document de rapport mensuel : ce document sera un référentiel sur lequel le service informatique se basera pour transmettre un rapport mensuel des incidents.
- Plan de sensibilisation et de formation : le document le plus important quand il s'agit de sécuriser un SI. En effet, le premier risque quand on parle de risque informatique reste le risque humain. Et c'est par la sensibilisation et la formation des collaborateurs aux différents risques qu'ils peuvent rencontrer qu'on peut éviter la plupart des attaques.
- Document du cycle PDCA : c'est un document avec lequel je détaillerai l'intérêt de chaque phase dans le cadre de l'amélioration continue du SMSI.
- Rapport de projet : c'est le document qui attestera de la progression du projet, et c'est également dans celui-ci que j'estimerai le ROI du projet.

Étude fonctionnelle

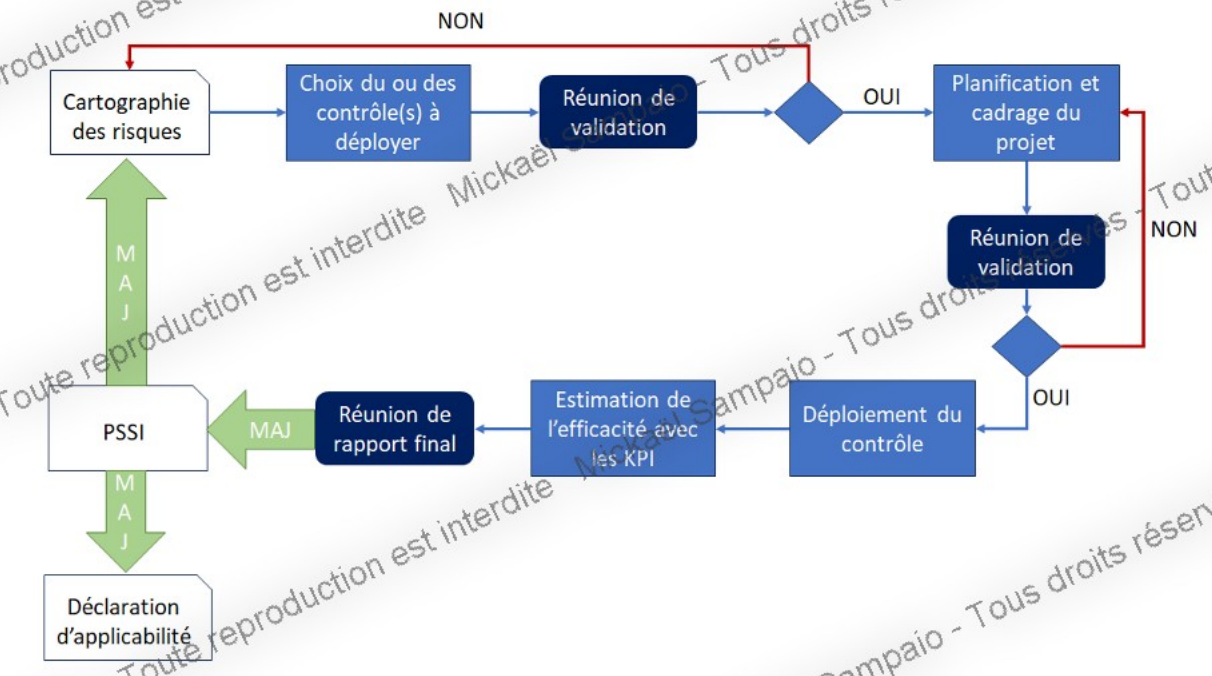
Ce projet est bien trop conséquent pour être réalisé d'un bout à l'autre dans son entièreté, et il est sûr qu'il devra être repris par Florian VERON dès mon départ. J'ai choisi en conséquent des méthodes de conduite de projet pour permettre à la bonne transmission du projet. D'autant plus que Florian n'a pas encore les compétences et les connaissances en termes de gestion de projet, et que c'est dans la formation en alternance qu'il intégrera en septembre qu'il découvrira toutes les notions et concepts de la gestion de projet.

Conduire le projet avec l'agilité

Vu la complexité et la charge de travail qu'il sera à effectuer pour déployer un SMSI au sein de PHILIANCE, j'opte pour conduite du projet basé sur l'agilité.

En effet, il sera bien plus pertinent de découper le projet et d'intégrer le SMSI brique par brique sur les catégories clés à sécuriser et qui rapporterait donc un maximum de valeur quant à la sécurisation d'un actif critique.

J'ai donc prévu un plan qu'il faudra respecter dans la conduite du projet pour permettre de réaliser le SMSI petit à petit, composant par composant, en se concentrant sur les risques majeurs.



: Représente un choix qui découle de la validation ou non de la Direction

MAJ : Représente la mise à jour d'un document

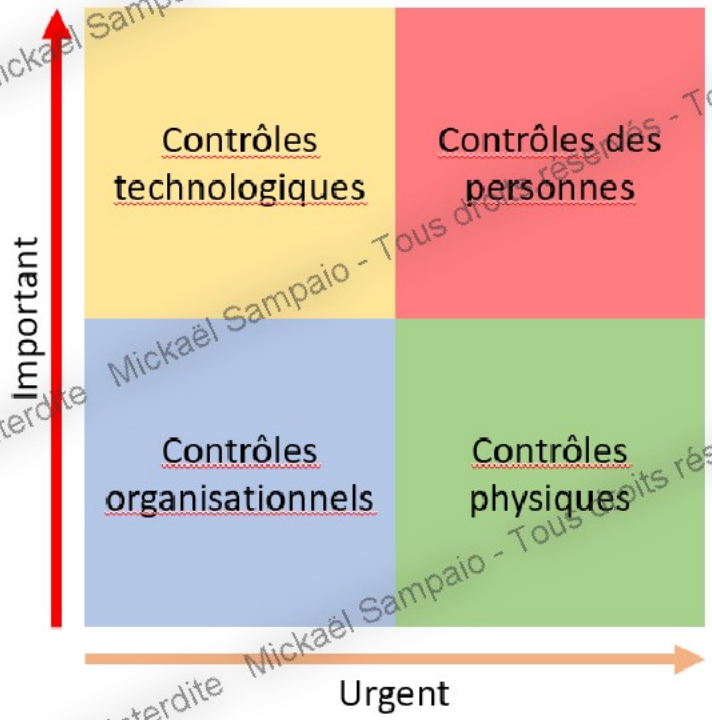
Matrice d'Eisenhower

Je dois avoir une représentation graphique efficace et simple pour représenter les différents besoins auxquels le SMSI doit répondre et également les prioriser si possible.

J'ai décidé de réaliser une matrice d'Eisenhower pour visualiser globalement les besoins de sécurité et pouvoir également les prioriser.

Je me base sur l'annexe A de l'ISO 27001:2013 pour avoir les différentes catégories d'une organisation à contrôler, car je n'ai pas accès à l'ISO 27001:2022 sur la bibliothèque ENI.

💡 **Je précise l'ISO 27001:2013 car celle-ci divise les catégories en 14 domaines, tandis que l'ISO 27001:2022 divise les catégories en 4 domaines.**[12]



Selon moi, le plus important et le plus urgent et d'appliquer des mesures de contrôles des risques sur le personnel. À savoir la planification de formation et de sensibilisation aux risques.

Car il est bien connu que la première faille de sécurité est causée par une action humaine, à savoir un utilisateur non averti sur les risques de sécurité.

Appliquer des mesures de contrôles technologiques est également très important, cependant il est préférable d'attendre la refonte du système informatique qui est prévu par la suite.

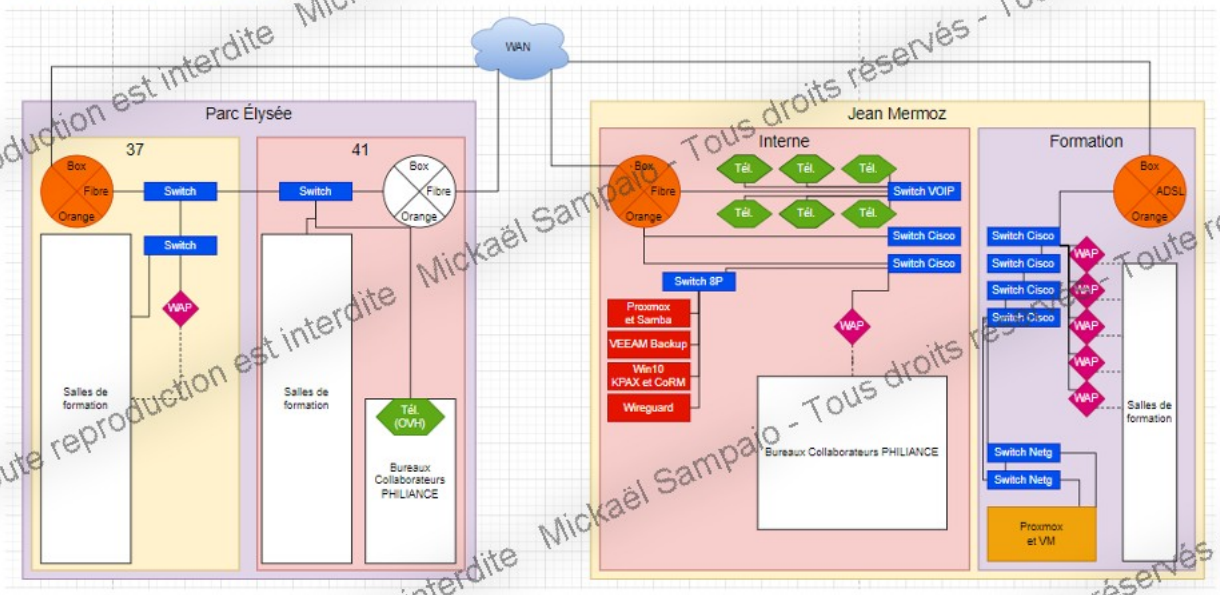
[12] « La norme ISO 27001 : Quels sont les changements à prévoir avec la version 2022 ? » tenacy.io, lien : https://www.tenacy.io/resources/norme-iso-27001-version-2022/

Les contrôles physiques sont quant à eux urgent à mettre en place mais cela ne revêt pas une criticité majeure dans le sens où après avoir publié la PSSI qui donnera les rôles et responsabilités de chacun, et après avoir formé et sensibilisé les collaborateurs sur les risques, je pense que les collaborateurs comprendront les risques qui sont liés aux accès physiques de leurs postes de travails, leurs bureaux, et surtout au local où sont situés physiquement les serveurs.

De plus, les locaux sont équipés d'affiches interdisant l'accès au public, et le local où sont situés les serveurs est verrouillé. Enfin, l'entièreté du bâtiment est sous vidéo surveillance.

Enfin les contrôles organisationnels seront mis en place progressivement au fur et à mesures de l'application des autres contrôles. Par exemple, pour la partie du SMSI que j'ai mis en place, et qui se concentre sur les contrôles des personnes, j'ai dû rédiger une PSSI, un accord de consentement éclairé, un document de cycle PDCA pour valider la démarche d'amélioration continue de la sécurité du SI. Ces documents font partis du contrôle organisationnel exigé dans l'annexe A de l'ISO 27001 :2022.

Schéma réseau



Le réseau n'étant pas cloisonné et ne présentant aucune configuration notable, on peut simplement le représenter en ayant une vision très globale.

Tous les switches (représentés par rectangle bleu) sont sur des valeurs d'usine ou non configurable.

Les icônes isocèles violettes nommées WAP représentent des points d'accès Wifi (Wifi Access Point).

Dans le bâtiment Jean Mermoz, deux sections bien distingues sont représentées, la section « Interne » et la section « Formation ». Cela permet de représenter les deux réseaux distincts n'ayant aucune communication possible entre eux car les réseaux sont distribués via deux box distinctes.

Dans le Parc Élysée, deux sections sont représentées, la section « 37 » et la section « 41 ». Ce sont deux locaux séparés dans un même bâtiment, cependant leurs réseaux communiquent ensemble car il y a un câble RJ45 qui relie les deux armoires de brassages. De plus, l'icône blanche « Box Fibre Orange » représente une box Orange qui est destinée à être retiré pour laisser une seule box distribuer internet aux deux locaux.

Classification des données

Avant de faire la cartographie des risques, il faut identifier et classifier les données selon leurs criticités du point de vue des critères de DIC (Disponibilité, Intégrité, Confidentialité).

Pour faire cette classification, j'ai listé les différentes données qui sont traités chez PHILIANCE et qui serait susceptibles de causer un risque.

À la suite de ce listing, j'ai organisé une réunion avec le service informatique pour que nous puissions tous estimer de l'impact que pourrait causer une donnée si le principe de DIC n'était pas respecté pour ladite donnée.

L'intérêt de réaliser cette estimation à plusieurs et d'avoir un résultat objectif.

Cependant, par expérience je sais que discuter d'un sujet aussi intéressant avec des passionnés amène de façon certaine de longs débats. Pour éviter ça, j'ai préparé une session de poker planning en ligne[13] où chacun doit mettre une estimation de criticité selon les critères DIC sur chaque groupe de données, et surtout, avec un temps imparti. Ainsi on évite des débats qui bien qu'intéressant peuvent grandement ralentir la phase de classification des données, et on a un résultat censé être objectif.

On peut voir le résultat de la classification des données ci-dessous :

Ref données	Types de données	D	I	C	Critère max
ACT.DON.FORM	Formation (BRS, planning)	2	2	2	2
ACT.DON.PII	PII sensibles (ID PE, CNI, Adresse)	2	3	4	4
ACT.DON.RH	Ressources Humaines (Contrats, salaires)	3	3	4	4
ACT.DON.MARK	Marketing et communication	2	1	3	3
ACT.DON.FIN	Finance (Bons de commande, Factures)	2	4	3	4
ACT.DON.IT	Informatique (Schémas d'infra, logins)	3	2	4	4

[13] Poker planning en ligne, lien: https://planningpokeronline.com/

J'ai choisi d'attribuer une référence à chaque type de données si toutefois je dois faire référence à celles-ci dans d'autres documents.

Je vois que selon les estimations, les données PII, RH, financières et informatique sont les plus sensibles, avec les données financières nécessitant des mesures pour préserver l'intégrité, et les trois autres nécessitant des mesures pour préserver la confidentialité. Quand je dis préserver l'intégrité ou la confidentialité, cela ne veut pas dire d'uniquement se concentrer sur ce critère de DIC, il est évident que quel que soit le critère DIC le plus critique, il faut si possible appliquer des mesures de disponibilité, d'intégrité et de confidentialité de l'information.

Cette classification des données m'ont été utiles pour l'étude technique où j'ai dû tenir comptes des données les plus critiques pour appliquer des mesures appropriées.

Cartographie des risques

Pour cartographier les risques, il faudrait dans l'idéal effectuer une recherche documentaire pour analyser les plus gros risques qui ont impactés des organismes de formations semblables à PHILIANCE, il faudrait réaliser des réunions avec les différentes équipes pour que chacun puisse échanger librement sur les différents risques pour lesquels nous sommes exposés. De plus il est intéressant de faire une revue des incidents passés pour inclure les risques connus dans la cartographie.

Cependant avec une contrainte de temps, je préfère éviter d'avoir une approche où je vise une cartographie parfaite et complète, mais je préfère en réaliser une simple et listant les risques principaux et insister sur une revue régulière de la cartographie dans le cycle PDCA.

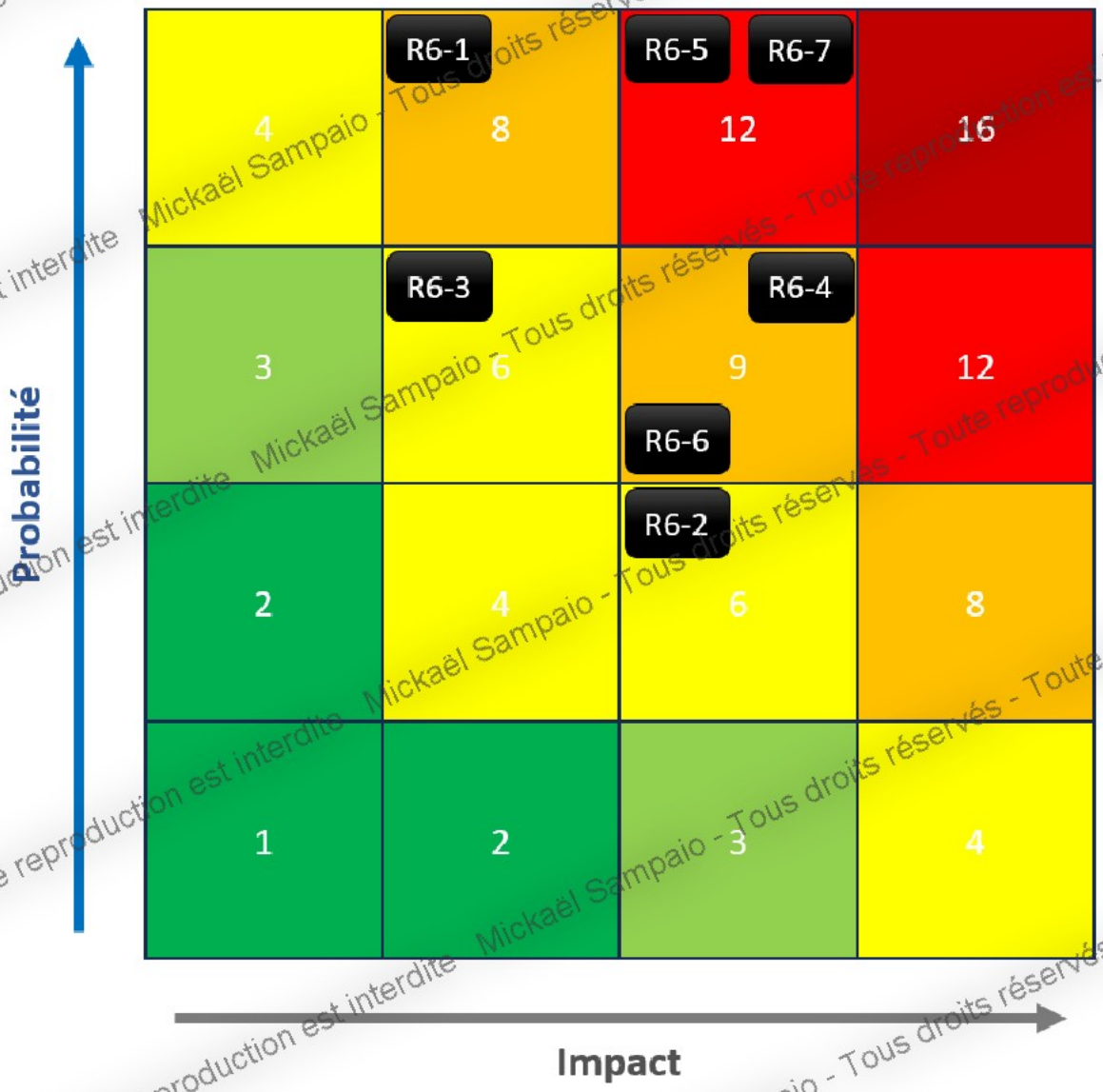
Pour réaliser cette première cartographie, je me suis concentré sur les risques causés par nos collaborateurs et principalement par leurs mauvaises connaissances des risques cyber. De plus, j'ai réalisé cette cartographie avec toute l'équipe du service informatique pour éviter des oublis et avoir un avis global objectif.

Tout d'abord, j'ai demandé les risques et nous avons estimé la probabilité qu'une activité malveillante provienne de ceux-ci ainsi que l'impact que cela peut causer :

Réf.	Risque	Probabilité	Impact	Criticité
R6-1	Accès non autorisé au poste (sur site et télétravail)	4	2	8
R6-2	Sabotage	2	3	6
R6-3	Transmission de données par inadvertance	3	2	6
R6-4	Partage des accès	3	3	9
R6-5	Utilisation de clé USB d'origine inconnue	4	3	12
R6-6	Téléchargement de virus (phishing, site malveillant / non sécurisé)	3	3	9
R6-7	Enregistrement d'accès sur un support non approprié	4	3	12

La référence que j'ai choisi d'utiliser se base sur la première lettre « R » pour (R)isque, suivi de la référence de la catégorie des contrôles de l'annexe A de l'ISO 27001 :2022, à savoir dans ce cas précis, les contrôles qui seront à appliquer sont des contrôles humains (principalement la formation et la sensibilisation) qui sont référencés en 6ème catégorie dans l'annexa A.

À la suite de cette classification des risques, j'ai effectué une cartographie des risques :



Cette cartographie m'a permis de représenter graphiquement, et facilement les risques sur lesquels il est important de se concentrer dans l'application de contrôle de mitigation des risques.

En effet, sur ce graphique je vois bien que les risques estimés qui pourraient être les plus impactant pour PHILIANCE sont R6-5 et R6-7, donc l'utilisation de clé USB d'origine inconnue et les enregistrements d'accès sur des supports non appropriés.

De plus, je remarque que R6-1, R6-4 et R6-6 sont également en zone orange, il est donc également important de les réduire.

Plan de formation et de sensibilisation

Pendant toutes mes études, on m'a toujours dit que le principal risque est la personne devant son poste de travail. Cela m'a été confirmé pendant mes recherches. Avec une étude de Kaspersky qui confirme que 90% des failles proviennent d'erreurs humaines[14].

J'ai donc dû établir un plan de formation et de sensibilisation aux risques cyber.

Les actions à prévoir

Comme l'expliquait Ramadhan NDEGEYA, il faut au minimum deux jours de formations par an. Je vais me baser sur cette valeur qui me paraît cohérente. Cependant je pense qu'il faut également un processus continu de sensibilisation et de tests plus particulièrement, pour éviter que les collaborateurs reprennent leurs mauvaises habitudes après ces journées de formation.

Je prévois donc deux jours de formation dans l'année. Et je prévois des campagnes de tests qui seront à réaliser régulièrement.

Formation ponctuelle

Des demi-journées ponctuelles de formations sont indispensables pour sensibiliser et former les collaborateurs sur les risques, les responsabilités de chacun, et les pratiques à adopter pour mitiger les risques.

Je pense qu'il faut éviter de faire des formations trop longues pour réussir à captiver l'auditoire du début à la fin. J'opte donc pour une demi-journée de formation.

Il est important de communiquer en amont le jour de formation pour éviter la pose de congé, permettre aux collaborateurs d'organiser leurs plannings, etc… De plus, je pense qu'il faut également communiquer les sujets qui seront évoqués pendant la formation. Cela peut permettre aux collaborateurs d'aller en amont se renseigner sur lesdits sujets, et donc permettre une meilleure assimilation de l'information le jour J, et également si possible d'aller plus profondément dans les explications.

Pour ce qui est de la communication, il faut éviter de communiquer trop tard la prochaine demi-journée de formation, pour laisser le temps aux collaborateurs de s'organiser, mais il ne faut pas le communiquer trop tôt non plus, pour pouvoir adapter la formation sur les pratiques cruciales de sécurité qui sont les moins respectées au moment de faire la formation.

[14] Le facteur humain est un enjeu majeur de la cybersécurité en entreprise, Kaspersky, lien : https://media.kaspersky.com/fr/business-security/enterprise/Fiche-Kaspersky-Security-Awareness_Facteur-humain.pdf

J'estime que prévoir trois mois à l'avance la formation paraît juste.

De plus, voici un mail type que j'ai rédigé pour l'annonce :

Bonjour à tous,

Dans le cadre de la planification de formation et de sensibilisation continue prévue dans la Politique de Sécurité du Système d'Information, vous êtes convié à une demi-journée de session de formation aux risques cyber le Mercredi 15 Octobre 2023.

Groupe 1 -> 9h00-10h30 – 10h45-12h30
Groupe 2 -> 13h30-15h – 15h15-17h00
Vous trouverez en pièce-jointe une feuille Excel concernant les personnes conviées selon les groupes.

Le déroulement de cette demi-journée de formation :

- Comprendre les menaces et les risques
- Comprendre comment protéger l'information et son poste de travail
- Comprendre pourquoi il est important d'être impliqué dans la sécurité du SI
- Comprendre les responsabilités de chacun et les réglementations
- Comprendre les bonnes pratiques
- Quizz final

N'oubliez pas que **la coupe du collègue le plus sécure ainsi qu'un prix spécial** seront attribués en fin d'année, à la personne la mieux noté selon votre engagement pendant cette formation et selon votre implication tout au long de l'année dans la sécurité de PHILIANCE !

Petite astuce pour gagner des points facilement : Renseignez-vous en amont de la formation sur les points qui seront évoqués pour prouver votre engagement et faire en sorte d'explorer un maximum de choses pendant cette formation !

Cordialement,

PHILIANCE FORMATION

MICKAEL SAMPAIO
Apprenti Cybersécurité
2 rue Jean Mermoz – ZA St Guénault
Immeuble « ARC EN CIEL »
91080 COURCOURONNES
01.69.47.45.90

Dans ce mail je défini bien le jour et les horaires, et je défini également deux groupes, un pour le matin et un pour l'après-midi. Diviser la formation en deux groupes distincts est obligatoire pour ne pas cesser entièrement les activités pendant une demi-journée.

De plus, j'amène deux éléments qui sont très important pour assurer une cohésion collective dans l'implication à la sécurité. La compétitivité, et la récompense.

C'est un peu le principe de la carotte et du bâton. J'amène une récompense à la personne qui montrera son investissement à respecter les règles de sécurité définies. De plus, j'ajoute un

côté compétitif pour l'obtention de cette récompense. Et en France nous avons une culture de la compétition assez importante qui peut éveiller certaines mentalités.

Sensibilisation continue

Il est également intéressant de communiquer des informations sur l'état général des risques cyber auxquels on est régulièrement confrontés. Ça peut être un simple mail ou bien des affiches par exemple.

L'objectif étant de donner des informations choquantes, pour captiver l'attention, puis de donner des méthodes de préventions des risques, ou simplement rafraîchir la mémoire en rappelant des choses vues pendant les séances de formations.

Règles d'éthique et légale d'une simulation d'attaque

Je prévois également le déploiement de plateforme pour réaliser des tests de cyberattaque interne.

Avant de mettre en place cela, je me suis d'abord questionné sur le fait que ce soit légal ou pas. Et également, est-ce que cela respecte l'éthique et les codes de déontologie du métier.

D'un point de vue légal, je n'ai pas réussi à trouver d'information assez précises et fiables pour savoir à quel point un test peut s'approcher du réel. Donc je vais devoir adapter la PSSI pour indiquer que les campagnes de tests devront être étudiée en amont d'un point de vue juridique pour éviter tout problème légal.

De plus, il pourrait être intéressant à l'avenir d'avoir l'appui d'une expertise juridique pour savoir jusqu'où on a le droit d'aller dans les simulations.

De plus, il est important de contractualiser avec les collaborateurs le fait que le service informatique se réserve le droit de réaliser des simulations d'attaques dans le cadre de sensibilisation des collaborateurs.

D'un point de vue éthique et déontologique, je préfère qu'une simulation soit clairement annoncée, à savoir son début et sa fin, exposer clairement les intérêts bénéfiques de celle-ci, et de plus, je dois bien expliquer que le but principal est la sensibilisation et donc l'amélioration de la sécurité de PHILIANCE, et aucunement la surveillance ni la sanction. Il faut avoir une approche bienveillante, avec une entière transparence.

Étude technique

Pour faire suite à cette étude de faisabilité, je dois concevoir la stratégie pour développer une culture de sécurité au sein de PHILIANCE, et je dois déployer les méthodes et solutions pour répondre aux besoins de sécurité centrées sur l'humain.

Pour ce faire, j'ai quatre objectifs distincts :

- Rédiger une PSSI
- Définir un plan de formation
- Définir une méthode pour réaliser une sensibilisation continue
- Réaliser la matrice de risques résiduelle

De plus, afin de mesurer l'efficacité des actions, je dois prévoir des KPI pour chaque solution ou méthode implémenté.

Enfin, avec le schéma réseau, je vois clairement que, bien que celui ne présente pas de haute disponibilité, il est assez sécurisé car il y a un réseau bien distinct pour le personnel et les activités internes à PHILIANCE, et un réseau distinct pour les clients. La mise en sécurité du réseau peut donc être vue par la suite mais cela n'est pas une priorité contrairement aux contrôles du personnel.

Politique de Sécurité du Système d'Information

Pour m'aider à la rédaction de la PSSI, je me suis basé sur la PSSI de l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Informations, qui est publique[15]. Selon les objectifs, j'ai dû réaliser la première version de la PSSI en me concentrant uniquement sur l'aspect du personnel interne à PHILIANCE, et des méthodes de sensibilisations.

L'intérêt de la PSSI est d'annoncer clairement le ou les responsables des actifs informationnels et du SI, d'annoncer le champ d'application et tout ce qui est exclu de la politique, d'évoquer également les sanctions qui sont applicables en cas de non-respect de ladite politique et d'annoncer comment sont mises en place les mesures de sécurité.

💡 **La PSSI est indiquée comme un contrôle organisationnel dans l'annexe A de l'ISO 27001 :2022 mais j'estime qu'elle influe également dans la sécurité du personnel, car le personnel se devra de lire la PSSI et d'en comprendre les règles établis ainsi que leurs responsabilités dans le cadre de la sécurité du SI.**

[15] PSSIE de l'ANSSI, lien : https://www.ssi.gouv.fr/uploads/IMG/pdf/pssie_anssi.pdf

Champ d'application

Le champ d'application de la première version de la PSSI se concentrera principalement sur l'aspect humain et plus particulièrement sur les collaborateurs internes. Seront exclus les tiers à savoir les formateurs et délégataires, et les partenaires, Xonatis et Doranco notamment.

Je définis les collaborateurs internes comme « personnel » interne de PHILIANCE, étant des personnes qui utilisent tout ou partie du système d'information.

Objectifs

Les objectifs à mentionner sont :

- La mise en place de formations régulières du personnel.
- La présentation de l'existence du formulaire de consentement éclairé pour les collaborateurs qui peuvent être soumis aux tests.
- Le but des tests, et expliquer clairement que les tests ne servent pas à évaluer les collaborateurs mais à les sensibiliser.

Plan de formation

Bien que Ramadhan NDEGEYA indique qu'il faut au minimum deux formations par an, je pense que la Direction n'acceptera pas un investissement de temps aussi conséquent compte tenu du projet de refonte du système informatique qui nécessitera lui aussi un sérieux investissement.

J'ai donc préconisé au minimum une formation annuelle, mais qui devra être accompagnée par des campagnes de tests de cyberattaque pour renouveler régulièrement les bonnes pratiques à adopter et faire en sorte que les collaborateurs adoptent ces bonnes pratiques de manière constante.

Chaque formation devra se conclure sur un test, pour estimer l'assimilation des notions des collaborateurs, et faire en sorte :

- De diriger les campagnes de tests sur les points faibles.
- D'adapter les prochaines formations sur les points fiables.
- De renforcer les formations sur les collaborateurs ayant le plus de mal à appréhender la cybersécurité et les bonnes pratiques inhérentes.

Mesurer l'efficacité des actions de formation

Pour mesurer l'efficacité de l'action de formation, je prévois un quizz en fin de celle-ci. Les premières statistiques qu'on pourra en tirer ne seront peut-être pas pertinentes, néanmoins sur deux ou trois ans on pourra constater si les collaborateurs s'améliorent dans la compréhension des risques cyber.

Méthode de sensibilisation continue

Il est bien connu que la théorie est réellement assimilée avec la pratique, c'est pourquoi j'ai défini, en addition au plan de formation, une méthode pour sensibiliser et régulièrement raviver les esprits sur les risques cyber.

J'ai proposé différentes méthodes, comme des tests de phishing, des tests avec des clés USB éparpillées, des tests de DNS poisoning, ou simplement des quizz de rappel.

Cependant, pour réaliser ce genre de test il faut impérativement avoir l'accord de consentement éclairé des collaborateurs. C'est-à-dire qu'il faut expliquer en toute transparence l'intérêt des tests aux collaborateurs, expliquer que le but est la sensibilisation et non l'évaluation. Toutefois, même si l'intérêt n'est pas d'évaluer, cela reste important de réajuster les actions de formations en fonction des mesures faites. Par exemple, si Zakaria SAOUDI, qui est chargé de facturation, ne fait plus d'erreurs que les autres collaborateurs pendant les tests, il sera pertinent d'accentuer la formation à son égard.

J'ai donc rédigé un accord de consentement consultable en annexe 2.

Ce document, comme explicité dans la PSSI, sera à faire signer par chaque collaborateur avant chaque campagne de tests. Si un collaborateur ne le signe pas, alors celui-ci ne devra en aucun cas être soumis aux tests.

Inclure les KPI

Quel que soit le type de campagne de tests, les formations ou les méthodes de sensibilisation, j'ai précisé et préciserai dans chacun de mes documents qu'il faut en amont prévoir les KPI qui permettent de s'assurer de l'efficacité d'une action.

Pour les formations, se seront des quizz ou des tests qui mèneront à des notes finales.

Les campagnes de tests de cyberattaques doivent si possible permettre la visualisation sous forme d'un tableau de bord des différentes étapes de la cyberattaque et des actions des collaborateurs. Par exemple dans le cas d'une attaque par phishing, il faudra avoir le nombre de collaborateur qui clique sur le mail, qui clique sur le lien, qui entre les informations de connexions, etc…

De plus, même pour la suite du projet qui sera repris par Florian VERON, j'indique dans les documents de trame du projet que peut importe la mesure de contrôle qui est mise en place, il faut impérativement inclure des KPI.

Cycle PDCA

Le cycle PDCA est un modèle de la roue de Deming qui s'inscrit dans la démarche d'amélioration continue. J'aurai pu intégrer le processus d'amélioration continu sans pour

autant détailler le cycle PDCA, cependant, comme l'explique Nicolas MAYER dans sa publication, il est préférable de détailler et documenter au possible les processus inhérents au cycle PDCA pour améliorer la compréhension de cette méthode.

Je pense que même si le cycle PDCA est une démarche continue, il est bien de fixer des dates ou un certain temps entre chaque itération pour avoir une contrainte qui force à appliquer cette démarche. Je pense qu'une itération de 6 mois pour réaliser un cycle complet me paraît cohérent à appliquer par défaut, avec des ajustements en fonction des besoins.

Le document détaillant le cycle PDCA à adopter pour le SMSI se trouve en Annexe 1.

Matrice de risques résiduelle

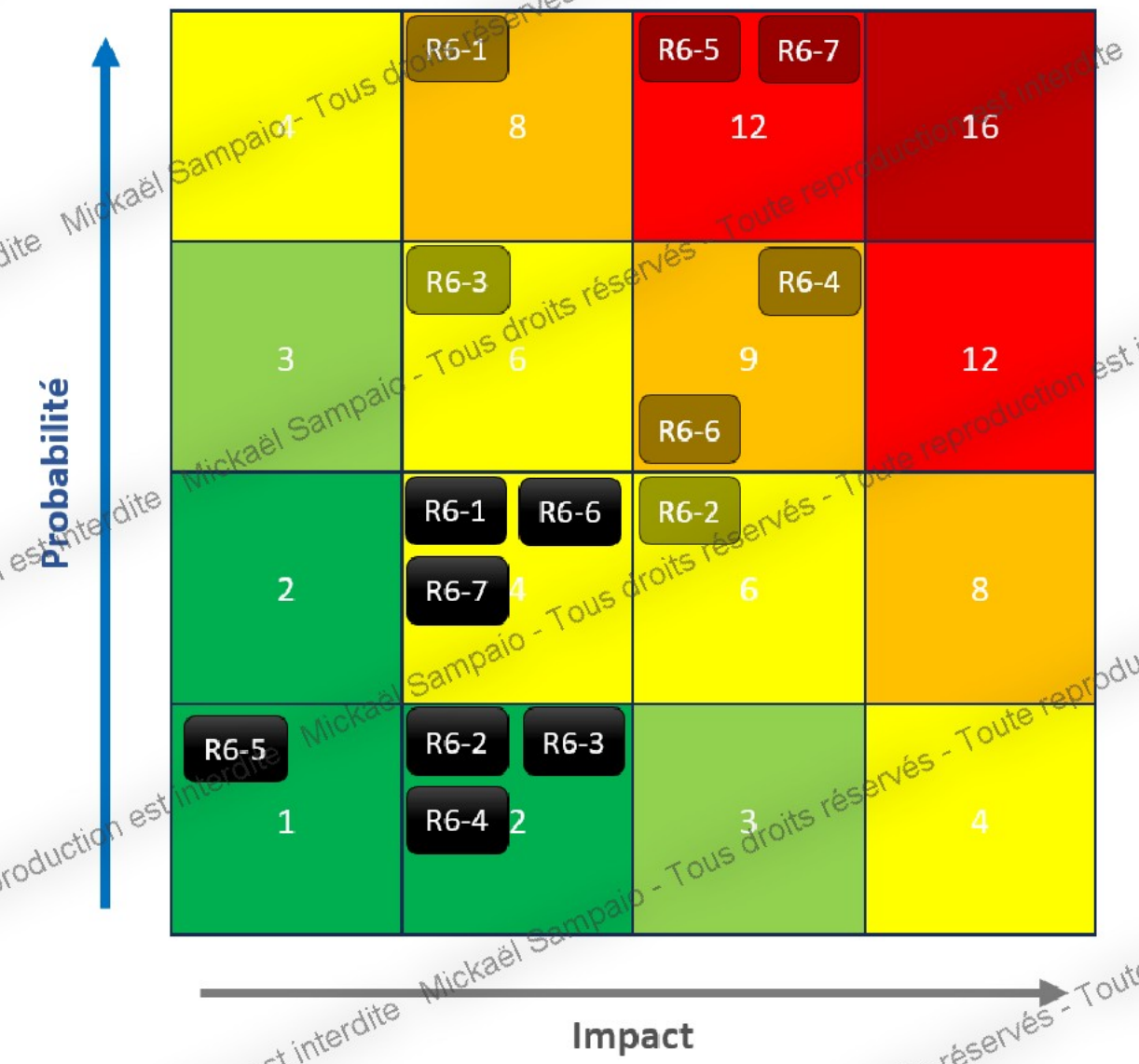
J'ai estimé une matrice de risques résiduelle qui permet de voir la diminution de la criticité des risques après avoir appliqué une mesure de mitigation. Cependant avant de réaliser celle-ci, j'ai besoin d'appliquer les mesures correctives aux dits risques tel quel :

Réf.	Mesure corrective	Probabilité Avant -> Après	Impact Avant -> Après	Criticité Avant -> Après
R6-1	Formation et sensibilisation, contrôles d'accès physique	4 -> 2	2 -> 2	8 -> 4
R6-2	PSSI, contrôles d'accès physique	2 -> 1	3 -> 2	6 -> 2
R6-3	PSSI, gestion des accès, formation et sensibilisation	3 -> 1	2 -> 2	6 -> 2
R6-4	Formation et sensibilisation, gestion des accès, PSSI	3 -> 1	3 -> 2	9 -> 2
R6-5	Formation et sensibilisation, contrôles techniques	4 -> 1	3 -> 1	12 -> 1
R6-6	Formation et sensibilisation, contrôles techniques	3 -> 2	3 -> 2	9 -> 4
R6-7	Formation et sensibilisation, gestion des accès	4 -> 2	3 -> 2	12 -> 4

Cependant, il faut que je garde à l'esprit que ce résultat est hypothétique, et se base sur une estimation où :

- Le personnel participe activement aux formations et assimile l'essentiel des risques et des bonnes pratiques.
- La formation est de bonne qualité et ludique.
- Les contrôles techniques sont efficaces.
- La définition des rôles et des responsabilités de chacun, ainsi que les sanctions, dans la PSSI sont bien définis et compréhensibles.
- Il y a un fort engagement de la Direction qui se propage également au personnel.

Enfin, je peux créer la matrice de risques résiduelles :



Risque tolérable	Risque majeur	Risque intolérable

J'ai donc l'estimation de la criticité des risques après applications des mesures correctives du SMSI.

Compte rendu du projet

Les objectifs atteints

Le principal objectif que je devais atteindre était d'impliquer la Direction dans la mise en sécurité du SI. Et cela devait découler à la mise en place d'un SMSI.

Cet objectif a été atteint, cependant la validation tardive du projet ne m'a pas permis de déployer le SMSI dans son intégralité.

En me concentrant sur l'aspect le plus important de la sécurité, à savoir les utilisateurs du SI, j'ai pu néanmoins rédiger les documents qui sont nécessaires à l'intégration de la sécurité dans le SI, à savoir :

- La PSSI, qui bien qu'à sa première version, se concentre principalement sur l'aspect humain.
- Un plan de formation qui permettra d'inculquer aux collaborateurs les bonnes pratiques de sécurité.
- Un accord de consentement éclairé, qui permettra d'effectuer des campagnes de tests de cyberattaque dans les règles.
- Un plan d'amélioration continue, qui permet d'engager la direction et le service informatique à appliquer une démarche d'amélioration continue du SMSI.
- Une cartographie des risques centrée sur les risques humains, qui permet d'avoir une visualisation pratique des risques qui sont les plus critiques et donc qui permet de concentrer les solutions de mitigation sur ceux-ci.

Ce qu'il reste à faire

Il reste encore beaucoup à faire, et c'est Florian VERON, qui occupera mon poste en alternance dès mon départ, qui reprendra le projet du SMSI.

Ce qu'il reste à faire représente encore un travail gargantuesque, à savoir :

- La mise à jour de la cartographie des risques pour prendre en compte les trois autres aspects de la sécurité : l'aspect organisationnel, l'aspect physique, et l'aspect technologique.
- La déclaration d'applicabilité si PHILIANCE souhaite à terme passer la certification ISO 27001.
- Adapter la PSSI pour inclure les domaines de la sécurité du SI restant.
- Créer les documents de PCA et de PRA.
- Réaliser une cartographie des processus.
- Conduire des projets centrés sur la mise en sécurité technologique.

Et c'est le dernier point que j'ai évoqué qui sera le plus lourd, car il nécessite des investissements, à la fois de temps comme financier très important.

Bilan professionnel et personnel

Bilan professionnel

Points positifs

Ce projet est gargantuesque, et au départ je ne me rendais pas compte de la charge de travail qu'il représentait. Pendant mon cursus scolaire j'ai été initié aux techniques et aux méthodes de gestion des risques. Cependant, un SMSI va bien au-delà de ça. C'est un engrenage de documents et de méthodes, mêlés à des pratiques de communications pour réussir à engager l'organisation et les personnes dans une démarche de sécurité. Et la façon de mener ce projet me semblait particulièrement abstraite. J'ai même encore à l'heure actuelle le même ressenti. Je pense en effet que j'aurai pu mener ce projet bien plus efficacement en ayant les conseils de quelqu'un qui a déjà mené ce projet.

Cependant, je suis certain que l'état de l'art que j'ai effectué, et les nombreuses heures de recherches et de lecture m'ont permis d'assimiler les notions les plus importantes pour mener un projet englobant autant l'aspect humain et ayant un impact aussi lourd dans une organisation.

Axe d'amélioration

Je pense que mon principal défaut est de ne pas aller en profondeur dans un sujet qui m'intéresse. Je suis bien trop curieux et j'aime découvrir de nouvelles façons de faire.

J'ai par exemple pendant mon état de l'art, découvert un principe d'architecture qui est l'urbanisation du SI. Ce concept m'était inconnu et bien que j'ai travaillé et effectué mes recherches sur un domaine que j'affectionne, j'ai été happé par ce nouveau sujet. À un tel point que j'ai acheté un livre, et j'ai finalement dévié de mon état de l'art pour étudier un nouveau sujet qui est tout autant complexe.

Heureusement que j'ai réalisé de moi-même que cette étude, bien qu'elle soit intéressante et utile pour ma carrière professionnelle, n'était pas une priorité et que je devais me recentrer sur mon mémoire.

Je pense qu'il faut que je travaille sur moi pour mieux me dédier sur l'apprentissage d'un sujet en particulier, et passer plus de temps à l'étudier en profondeur, plutôt que de développer sans cesse de nouvelles connaissances de surface.

Projet professionnel

Je suis quelqu'un de plutôt ambitieux et j'aimerai intégrer un poste d'assistant RSSI après mes études. Et je pense que ce projet qui m'a permis de traiter m'a problématique, mêlé à mes années d'études, m'ont apporté les connaissances nécessaires pour prétendre à ce poste.

Il me faut cependant garder en tête que pour occuper ce poste il me faudra être sans cesse en apprentissage en autodidacte, tant le monde de la sécurité informatique est vaste.

Bilan personnel

Avoir réalisé de longues années d'études en apprentissage, et conclure sur ce Master Networks & Security Manager en conduisant un projet conséquent et en effectuant un mémoire sur celui-ci m'ont appris plusieurs choses sur moi-même :

- Je préfère la qualité et la pérennité au détriment du développement et à la croissance rapide.
- Bien que j'ai un problème de confiance en moi, qui peut être une barrière conséquente dans un poste à responsabilité, celui-ci peut s'amoindrir en maîtrisant son sujet et en le partageant au bénéfice d'autrui.

De plus, en me reconvertissant dans l'informatique, je pensais initialement que je devais simplement suivre de longues années d'études où je devrais réellement m'investir continuellement jusqu'à obtenir mon Master. Et je pensais à tort qu'après l'obtention de celui-ci, je n'aurai plus besoin d'être autant investi. Mais j'ai l'impression que c'est tout le contraire. Et qu'au final, c'est maintenant que je devais devoir m'investir à fond dans ce qui me passionne pour pouvoir réellement apporter une valeur ajoutée dans les postes futurs que j'occuperais et dans la société, et apporter quelque chose qu'un autre ne pourrait pas.

Conclusion

Ce projet, bien qu'il ne soit pas fini, a été l'aboutissement de longues années d'études et il m'a permis de grandir aussi bien professionnellement que personnellement.

Professionnellement par les techniques que j'ai pu découvrir et appliquer, et par la masse d'information que j'ai pu accumuler qui sera cruciale pour ma carrière professionnelle.

Personnellement par la découverte que rien ne s'acquiert sans un réel investissement personnel, et par les bénéfices personnels que ce projet m'a apportés, où le côté humain et la communication sont la clé de la réussite.

Pour finir, ce projet n'aurait jamais pu être mené sans la bienveillance et la confiance que mes collègues m'ont apportée.

Merci.

Annexes

Annexe 1 : Démarche du cycle PDCA à adopter – Partie 1

Démarche PDCA à appliquer au SMSI

Qu'est-ce que le PDCA

Basée sur le principe de la roue de Deming, le PDCA est un cycle continue dont l'intérêt et d'apporter continuellement une amélioration à un service. Ce cycle comporte 4 phases : (P)lanifier, (D)eployer, (C)ontrôler, (A)gir.

Un cycle par semestre

Le début d'un cycle doit être initié de manière automatique et ne doit pas être décalé ni annulé sauf par la Direction. Il est prévu initialement qu'un cycle complet se base sur un semestre.

Planification

La phase de planification est la phase où les composants du SMSI seront analysés pour estimer les axes les plus pertinents qui pourraient améliorer la sécurité de l'information. Deux solutions par domaine de la sécurité ISO 27001 :2022[1] doivent être choisi.

Avec huit propositions de solutions à implémenter/améliorer, une réunion de cadrage devra être conduite par le responsable du SMSI avec la Direction pour choisir certaines des huit solutions qui seront à implémenter/améliorer.

Suite au choix, il faut réaliser une étude des différents outils ou méthodes pour satisfaire les besoins d'amélioration, puis planifier leurs déploiements.

Selon les solutions qui seront mises en place, il pourra être pertinent de définir un cahier de test qui servira dans la phase de contrôle à s'assurer que les besoins soient comblés.

La phase de planification ne doit pas durer plus de deux semaines.

Déploiement

La phase de déploiement, où on va mettre en œuvre la ou les solution(s) choisies.

La phase de déploiement ne doit pas durer plus de deux mois.

Contrôle

On évalue que les besoins sont comblés selon des mesures récoltées, fiables et vérifiables. C'est également à cette étape qu'on complètera le ou les cahiers de tests qui seront à faire valider par le responsable du SMSI et la Direction.

La phase de contrôle ne doit pas durer plus de deux semaines.

[1] Les 4 catégories de la sécurité selon l'ISO 27001 :2022 sont : Contrôles Organisationnels, Contrôles Physiques, Contrôles du Personnel, Contrôles Techniques

PHILIANCE FORMATION
Parc Elysée – 37 rue Anatole France
91080 Courcouronnes
☎01.69.47.45.00 @contact-ileDeFrance@philiance.com

Agir

C'est une phase d'action et on ajuste les solutions ci-besoin. Cette phase peut être continue jusqu'à l'envoie du rapport du cycle, c'est-à-dire jusqu'au 5ème mois.

Fin du cycle

Un rapport complet du cycle sera à transmettre à la Direction au 5ème mois. Une réunion avec la Direction sera conduite par le responsable du SMSI pour échanger et valider que le cycle ait bien été conduit et de sa valeur ajoutée.

Si la méthode du cycle PDCA est à revoir, c'est à la suite de cette réunion que les modifications seront actées et validées par le responsable du SMSI et la Direction avant la conduite du prochain cycle semestriel.

Historique des versions

Date	Auteur	Changements	Version
04/08/2023	M. SAMPAIO	Version initiale	1.0

PHILIANCE FORMATION
Parc Elysée – 37 rue Michel Ange
91080 Courcouronnes
01.69.47.45.00 @contact-iledefrance@philiance.com

Annexe 2 : Formulaire de consentement éclairé

Formulaire de consentement éclairé à une campagne de tests de cyberattaque

Je soussigné(e) NOM /Prénom : ..... atteste que le responsable de la campagne de tests de cyberattaque : ..... m'a délivré des informations claires concernant les tests qui me seront soumis pendant la période définie de : ..... à partir du : ..... / ..... / ..... jusqu'au : ..... / ..... / .....

J'ai été informé(e) :

- Des types de tests auxquels je pourrais être soumis(e) ;
- De l'intérêt des tests à me sensibiliser aux risques de sécurité informatique ;
- Que des méthodes de formation pourraient être accentuées à mon égard pour m'aider à mieux comprendre les enjeux de la sécurité et les risques auxquels je suis confronté(e) dans le cadre de mes activités quotidiennes.

J'ai également été prévenu(e) que cette campagne a pour unique but de me sensibiliser et me former aux risques, et qu'aucune sanction ni reproche ne me sera fait si je venais à échouer à un test.

Je reconnais avoir pu poser toutes les questions concernant cette campagne de tests et avoir compris les explications données en réponse.

Je m'engage à respecter les tests qui me seront soumis, à m'impliquer dans ceux-ci, et à ne pas les remettre en cause.

À Évry-Courcouronnes le : ...../...../ 2022

Signature précédée de la mention : « J'ai été informé(e) et consens »

PHILIANCE FORMATION
Parc Eiyeo – 37 rue Michel Ange
91080 Courcouronnes
01.69.47.45.00 @contact-ileDeFrance@philiance.com

Annexe 3 : PSSI – Partie 1

Politique de Sécurité du Système d'Information de PHILIANCE

Préambule

Cette présente politique de sécurité du système d'information de PHILIANCE contribue à :

- Assurer la continuité des activités de traitement de l'information
- Prévenir la fuite d'informations
- Augmenter la confiance des clients et des partenaires

Cette politique s'appuie sur des concepts inhérents à la gestion d'un système d'information et de la sécurité de celui-ci. En l'état actuel,

- Le système d'information est inscrit dans une démarche d'amélioration continue des services et de sa sécurité.
- Une planification de tout projet visant à inclure ou modifier des composantes du système d'information doit être réalisée en prenant en compte les ressources humaines et financières.
  La sécurité du système d'information se base sur des règles strictes de standards internationaux régissant les bonnes pratiques de gestion de la sécurité.
- Le personnel de PHILIANCE doit être informé de ses droits et devoirs mais également formé et sensibilisé à la cybersécurité et aux bonnes pratiques de l'utilisation du système d'information et des traitements de l'information.
- La mise en sécurité des données considérées comme sensibles sera adaptée et renforcée selon leurs besoins d'intégrité, de confidentialité, et de disponibilité.

Enfin, cette politique s'adresse tout particulièrement au personnel interne de PHILIANCE, mais est rendue publique sur le site représentant l'organisme PHILIANCE.

Article 1 : Champ d'application

La PSSI s'applique au système d'information de PHILIANCE, c'est-à-dire aux systèmes, logiciels, plateformes web externes, services Cloud, mais également aux locaux hébergeant ces composantes et à toute personne administrant ou utilisant tout ou partie dudit système d'information.

Article 2 : Date d'entrée en vigueur

La présente PSSI entre en vigueur le jour de son exposition publique sur le site représentant l'organisme PHILIANCE.

Article 3 : Pilotage de la PSSI

La PSSI sera revisitée et améliorée pour élargir son application sur des catégories de la sécurité de l'information bien spécifique, et pour renforcer les activités de mise en sécurité selon les études de risques préalables.

PHILIANCE FORMATION
Parc Elysée – 47 rue Michel Ange
01080 Courcouronnes
☎01.69.87.45.90 @contact-iledefrance@philiance.com

Toute modification sera rédigée par le référent interne de la sécurité de l'information et validé par la Direction avant publication.

La mise en application des directives de mise en sécurité sera réalisée par l'équipe interne responsable de la sécurité de l'information, mais pourra également s'appuyer sur des consultants ou prestataires externes qualifiés et validés par la Direction et le représentant interne de la sécurité de l'information.

Politique de formation et de sensibilisation du personnel

Planification de formation du personnel

PHILIANCE s'engage à fournir des formations en interne du personnel manipulant des composantes du système d'information.

Le responsable de la sécurité de l'information devra planifier la formation et les différents sujets qui seront abordés en fonction des résultats des formations et des campagnes de sensibilisations précédentes. De plus, la Direction validera cette action de formation avant d'engager toute action concrète visant à exécuter ladite formation.

Au minimum une formation d'une demi-journée doit être effectuée par an pour chaque personne.

Au minimum deux sessions de formation doivent être organisées pour permettre un roulement du personnel et éviter l'interruption totale des activités.

Une personne conviée à une formation est dans l'obligation d'y assister.

La date de la formation sera communiquée au moins 6 mois en amont pour permettre à chacun des acteurs d'anticiper cette journée et éviter toute perturbation dans les activités de chacun. Si un des membres du personnel ne peut pas être présent, alors c'est au responsable de la sécurité de l'information de planifier la session à un autre jour.

La formation doit être réalisée soit par un interne étant qualifié sur le sujet de la cybersécurité ou par un externe qui est qualifié et qui sera au préalable validé par la Direction.

Un test à la fin de chaque session de formation sera soumis pour s'assurer de la bonne assimilation des bonnes pratiques et des risques liés à la sécurité informatique. Le test aura pour unique objectif d'adapter les formations suivantes pour les personnes ayant le plus de difficultés à appréhender la cybersécurité et/ou sur les concepts les moins bien compris du public.

Sensibilisation continue du personnel

Des campagnes de sensibilisation du personnel devront être menées régulièrement.

Les objectifs d'une campagne seront :

- De renforcer la vigilance du personnel face aux cyberattaques
- De tester les réactions du personnel face à une cyberattaque.
  D'adapter les prochaines actions de formations en fonction des résultats de la campagne.
- De permettre une meilleure estimation des risques dans le cadre de projet de sécurisation du système d'information.

Le personnel devra donner son accord sur le « formulaire de consentement éclairé » avant d'être soumis aux tests.

PHILIANCE FORMATION
Parc Dyvée – 37 rue Michel Ange
91080 Courcouronnes
☎01.69.47.45.90 @contact-ileDeFrance@philiance.com

Annexe 3 : PSSI – Partie 3

Aucun test ne sera soumis au personnel n'ayant pas été informé de la campagne de test, des objectifs de celle-ci et n'ayant pas signé le « formulaire de consentement éclairé ».

Une communication générale de la campagne de test devra être réalisée afin que l'intégralité du personnel ait connaissance :

- Des types de cyberattaques auxquels ils pourraient être soumis.
- De la durée de la campagne, c'est-à-dire de son début et de sa fin.
- Du ou des objectifs précis de la campagne

Une campagne de test devra en aucun cas amener à la déstabilisation d'une composante du système d'information et ne devra en aucun cas altérer des données hébergées au sein du système d'information.

Les règles de déontologie et d'éthique inhérentes à la formation et la sensibilisation, à la gestion et à la sécurité de l'information guideront en tout temps la planification et l'exécution de la campagne de test.

Le responsable de la sécurité de l'information se portera garant du bon respect des lois et des réglementations quant aux tests de cyberattaques qui seront exécutés en interne, avec l'appui d'une expertise juridique ci-besoin.

Sanction

Tout utilisateur enfreignant cette politique et ne respectant pas ses devoirs est passible de sanction disciplinaire, pouvant aller jusqu'au licenciement.

De plus, tout membre du personnel ne respectant pas les règles et les bonnes pratiques de sécurité vues en formation est passible de blâme.

Historique des versions

Date	Auteur	Changements	Version
04/08/2023	M. SAMPAIO	Version initiale	1.0

PHILIANCE FORMATION
Parc Elysée – 47 rue Michel Ange
01080 Courcouronnes
☎01.69.47.45.90 @contact-ileDeFrance@philiance.com