Région îledeFrance

MASTER SIC
EM SORBONNE

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE
ÉCOLE DE MANAGEMENT
DE LA SORBONNE

Université Paris 1 Panthéon - Sorbonne

Mémoire de MASTER M2

SYSTÈMES D'INFORMATION ET DE CONNAISSANCE

sous-parcours **Business Analysis**

Promotion 2024-2025

« Piloter et intégrer les exigences de cybersécurité dans un contexte organisationnel complexe et fragmenté. »

RÉDIGÉ ET SOUTENU PAR : Marie-Caroline de la Barre de Nanteuil
DIRECTEUR DE MÉMOIRE : Samuel Parfouru
DATE DE SOUTENANCE : 01/10/2025

L'UNIVERSITE N'ENTEND DONNER AUCUNE APPROBATION
NI IMPROBATION AUX OPINIONS ÉMISES
DANS CE MÉMOIRE :
CES OPINIONS DOIVENT ETRE CONSIDÉRÉES
COMME PROPRES À LEUR AUTEUR

Résumé

Ce mémoire porte sur le pilotage des exigences de cybersécurité dans un contexte organisationnel fragmenté et marqué par un manque d'assimilation des procédures pour les chefs de projets, garants de la conformité des projets numériques. Cette étude a été réalisée dans le cadre d'une étude de terrain au sein du Conseil régional d'Île-de-France.

La question de recherche qui guide ses travaux est la suivante : *Comment piloter efficacement les exigences de cybersécurité dans un contexte organisationnel marqué par le manque de clarté, la fragmentation ou le manque de procédures structurées ?*

Mon étude s'appuie sur une année d'alternance au sein de la DSI de la Région, complétée par des entretiens menés auprès des chefs de projet, des référents conformité, de consultants externes ainsi qu'auprès du RSSI.

Cette analyse met en évidence les difficultés rencontrées lors du cycle de vie des projets numériques : la dépendance aux experts, la faible lisibilité des processus, la complexité des normes à respecter ainsi que le manque d'acculturation aux enjeux cyber.

A partir de ces différents constats, mon mémoire propose un kit de pilotage structuré et articulé autour de plusieurs étapes clés, visant à rendre les exigences de sécurité plus accessibles aux chefs de projet.

L'étude confirme ainsi l'hypothèse selon laquelle une formalisation claire et progressive des exigences ainsi qu'une sensibilisation continue, formerait une réponse adaptée pour répondre à cette problématique.

Remerciements

Je tiens tout d'abord à remercier Monsieur Denis MAZZALI de m'avoir accueillie au sein de son équipe et d'avoir été un tuteur bienveillant, m'accompagnant avec attention tout au long de mon alternance au sein du Conseil régional d'Île de France.

Je tiens à souligner l'aide précieuse apportée par Matthias FONTAINE, Responsable de projets Donnée et Gouvernance et Nathalie BUFFOTOT Directrice de projet, protection des Données et conformité Data et IA, pour leur accompagnement et leurs conseils avisés tout au long de la rédaction de ce mémoire.

Je souhaite également exprimer ma gratitude envers Monsieur Samuel PARFOURU, mon Directeur de Mémoire, pour le suivi attentif de mon travail tout au long de cette année et pour la confiance qu'il m'a accordée dans l'avancée de mes recherches. Je le remercie également pour la richesse de ses enseignements dispensés dans le cadre du module *Management des connaissances organisationnelles.*

Je souhaite témoigner ma profonde reconnaissance à Madame Selmin NURCAN et Madame Benedicte CARDIET-TREPS pour la confiance qu'elles m'ont accordée lors de mon intégration dans ce master, ainsi que pour la qualité des enseignements qui ont profondément conforté mon choix d'orientation.

Je n'oublie pas mes camarades de promotion pour le soutien mutuel précieux que nous avons su nous apporter dans les moments difficiles.

Finalement je remercie chaleureusement ma famille ainsi que Monsieur Grégoire de ROLLAND, Madame Zoé SOUCHET et Monsieur Théotime POICHOTTE de m'avoir soutenue et épaulée avec acharnement.

Table des matières

Tables des Illustrations

Introduction générale

A l'issue de mon parcours en Droit, Economie, Gestion au sein de l'Université Paris 1 – Panthéon Sorbonne, j'ai décidé d'opérer une réorientation afin de me tourner vers le domaine des systèmes d'information, convaincue de l'importance stratégique de la transformation numérique au sein des organisations. C'est dans cette optique que j'ai intégré le Master 2 Management des Systèmes d'Information, parcours Business Analysis, au sein de l'Université Paris 1 – Panthéon Sorbonne.

Parallèlement à cette formation, j'ai rejoint le Conseil régional d'Île-de-France en tant qu'alternante intégrée au Bureau projet, structure en charge de l'accompagnement de la coordination des projets numériques. Cette expérience enrichissante m'a permis d'intervenir sur des projets variés, de contribuer à la prise en compte des exigences des différentes verticales et également de veiller à la conformité réglementaire des projets portés par le Pôle transformation numérique.

C'est au fil de ces missions que j'ai découvert un véritable attrait pour la cybersécurité. Au fil du temps elle m'est apparue comme une discipline stratégique à la croisée de la gouvernance, des réglementations et de la conduite de projet. Ma position transverse m'a confrontée aux difficultés de traduire des obligations complexes en exigences opérationnelles. Cette prise de conscience a nourri ma véritable appétence pour ce domaine et a conforté ma volonté d'inscrire mon projet professionnel dans la stratégie de cybersécurité.

C'est dans cette logique que s'inscrit mon mémoire : analyser les enjeux liés à l'intégration des exigences de cybersécurité dans la gestion de projet et proposer des pistes d'accompagnement adaptées au contexte particulier des collectivités territoriales confronté à la densité réglementaire et organisationnelle. La problématique est donc la suivante : *Comment piloter efficacement les exigences de cybersécurité dans un contexte organisationnel marqué par le manque de clarté, la fragmentation ou l'absence de procédure structurée ?*

Afin de répondre à cette question, mon mémoire s'articule autour de quatre parties. La première partie présentera le contexte de mon mémoire afin de mettre en lumière l'environnement du Conseil régional d'Île-de-France et une courte introduction à la cybersécurité. La deuxième

partie développe ma revue de littérature autour de trois axes : le pilotage des projets numériques, la cybersécurité et l'intégration des exigences de cybersécurité. La troisième partie relate mon étude de terrain à travers des entretiens menés auprès des agents de la région Île-de-France. Et enfin dans un quatrième chapitre, je proposerai des pistes de solution et un dispositif d'accompagnement permettant de soutenir à long terme les chefs de projet dans l'intégration des exigences de cybersécurité. En effet les exigences de cybersécurité vont largement augmenter et notamment avec l'implémentation de la NIS 2, la nouvelle directive qui vise à encadrer et guider davantage les organisations dans l'implémentation de leurs mesures de sécurité. Il devient donc essentiel d'accompagner au mieux ces nouvelles contraintes venant s'ajouter à un contexte déjà bien complexe.

PARTIE 1 – CONTEXTE ET PROBLEMATIQUE

Les collectivités territoriales s'inscrivent dans le mouvement global de digitalisation présent dans tous les secteurs. Cette dynamique de modernisation entraine l'apparition de nouveaux outils et nouveaux usages. Si cela s'avère largement bénéfique pour les entreprises, cela entraine une interdépendance renforcée entre les technologies et les missions du service public dont est investie le Conseil Régional. Les innovations technologiques s'accompagnent de régulations plus denses et d'une nouvelle exposition aux risques cyber de plus en plus importante. Cela induit des changements tant organisationnels que techniques au sein des organisations.

Pour répondre à ces défis modernes, les collectivités doivent professionnaliser la gestion de leurs projets numériques et cela implique l'intégration constante des dimensions règlementaires et sécuritaires.

1. Contexte

1.1. Présentation de l'entreprise

Mon mémoire s'inscrit dans le cadre d'une mission réalisée au sein du Conseil régional d'île de France. Installé à Saint Ouen, cette institution politique majeure, investie pour le bien-être des franciliens, intervient dans la gestion et le bon fonctionnement du territoire. Elle s'implique par la planification, l'aménagement du territoire, le développement économique régional et l'appui aux projet numériques territoriaux. Acteur public de premier plan, elle est notamment reconnue pour son investissement dans les lycées publics d'île de France ainsi que la RATP.

Figure 1: Les services de la Région Île de France (iledeFrance.fr, 2025)

1.1.1. Intérêts des Collectivités

L'article L4433-1 du code général des collectivités territoriales définit précisément leurs rôles au sein de leurs régions : *« Le Conseil régional règle par ses délibérations les affaires de la région dans les domaines de compétences que la loi lui attribue.*
Il a compétence pour promouvoir le développement économique, social, sanitaire, culturel et scientifique de la région, le soutien à l'accès au logement et à l'amélioration de l'habitat, le soutien à la politique de la ville et à la rénovation urbaine et le soutien aux politiques d'éducation et l'aménagement de son territoire, ainsi que pour assurer la préservation de son identité et la promotion des langues régionales, dans le respect de l'intégrité, de l'autonomie et des attributions des départements et des communes. »

La collectivité territoriale est donc une autorité publique distincte de l'Etat. Chaque collectivité est dotée d'un exécutif et d'une assemblée délibérante élue au suffrage universel. Celles-ci exercent librement leurs prérogatives en complément de l'action de l'Etat.

1.1.2. Budget de la Région île de France

La région Ile de France gère donc un budget de 5 milliards d'euros par an, la majorité provenant de l'Etat. Ce budget lui permet d'agir dans de nombreux champs de la vie quotidienne des franciliens tels que les lycées, le développement économique, les transports, la formation, la culture…

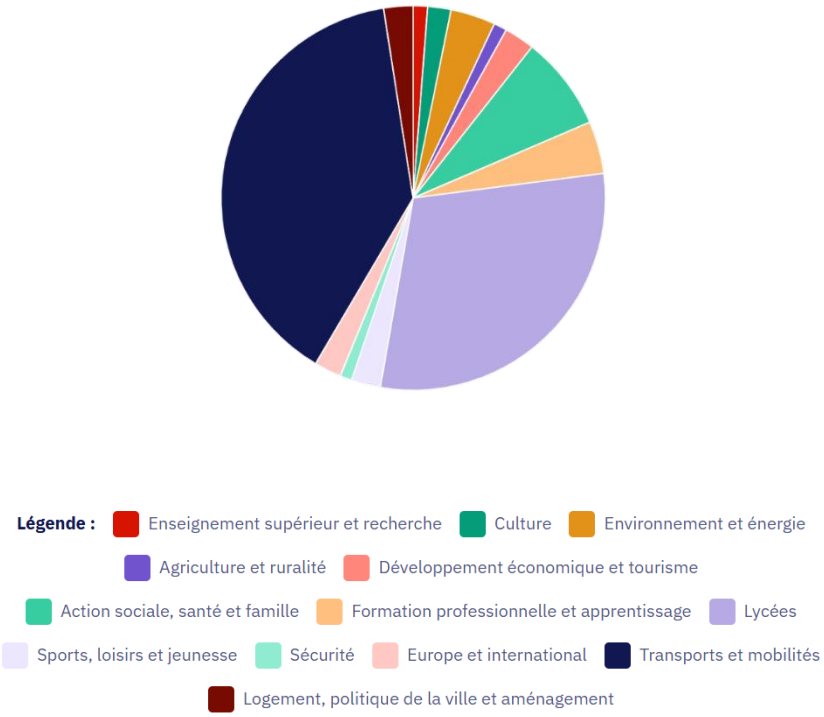

Figure 2 : Répartition du budget 2025 de la région (IledeFrance.fr, 2025)

1.2. La numérisation des collectivités

Les collectivités territoriales ont connues une accélération significative de l'augmentation de la numérisation ces dernières années. En effet, comme de nombreuses organisations, elles sont portées par les besoins d'efficacité permis par le numérique, et les nouvelles attentes des citoyens. Cette transformation vient toucher tous les niveau d'une organisation. Les outils se digitalisent, les services publiques interviennenent désormais en ligne et les données territoriales sont exploitées pour mieux piloter les politiques locales. Cette dynamique impose cependant de nouveaux défis en matière de cybersécurité, de formation ou encore de facture numérique.

1.2.1. Une Opportunité pour l'amélioration des services publics

La transformation numérique est aujourd'hui un levier majeur pour toutes les organisations publiques ou privées. Pour les collectivités terrritoriales, en plus d'être une modernisation technologique, elle resprésente une opportunité profonde de refonte des modes de gestion publique en améliorant notamment la qualité des services rendus aux citoyens et franciliens, aux entreprises et aux agents territoriaux.

1.2.2. Création du PTNUM face à la montée en charge des projets numériques

C'est face à ce contexte de numérisation accélérée que le Conseil régional d'Ile de France a entrepris en 2022 une réorganisation stratégique de ses différentes fonctions numériques. C'est ainsi qu'est né le Pôle Transformation Numérique, une structure centrale à laquelle est rattachée la Direction du Numérique, la Direction de la Donnée et la Direction des Systèmes d'Information, dans le but de piloter et structurer les projets numériques de façon transversale et sécurisée.

1.2.2.1. Un besoin structurel

Historiquement, la conduite des projets numériques au sein de la Région était fragmentée entre différentes directions métiers notamment la DSI et certains prestataires externes. Cependant ce fonctionnement en strates ne suffit plus face à la croissance fulgurante des projets : dématérialisation des services aux usagers, plateformes collaboratives, modernisation des infrastructures ou encore mise en conformité aux nouvelles réglementations. La création du Pôle Transformation Numérique visait à renforcer la gouvernance et l'accompagnement des projets numériques. Il a permit également de professionnaliser les pratiques de gestion de projet pour ensuite intégrer les différentes exigences essentielles (sécurité, RGPD, accessibilité…) dès les phases de cadrage en amont des projets. Les différentes exigences sont donc toutes liées au sein d'un même pôle à travers des référents qui assurent une collaboration restreinte avec les chefs de projets.

Cette nouvelle unité est donc composée de trois directions, elles même composées de sous-unités :

La direction des systèmes d'information : « *La Direction des Systèmes d'Information assure le pilotage des projets informatiques, techniques et bureautiques, gère le parc informatique et son environnement, définit et exploite les infrastructures techniques de communication et de télécommunication et assure le fonctionnement et la maintenance des logiciels, progiciels et services.* » [Document interne, Région Île de France, 2025]
Elle est composée de trois services et d'une mission :

- La mission « Sécurité et urbanisation » qui a pour périmètre la prise en charge des normes applicables (notamment concernant la prévention des risques) ainsi que la mise en place de la politique de sécurité. Cette mission cartographie les systèmes d'information, réalise les scénarios de simplification et garantit les bonnes pratiques SI.

- Le service « Infrastructure et production » qui a pour périmètre l'élaboration et la mise en œuvre de l'architecture informatique de la collectivité, la définition des conditions de rétablissement de l'activité informatique en cas de sinistre majeur. Ce service garantit la cohérence de l'infrastructure technique du système d'information et assure la mise en œuvre des infrastructures réseaux et sécurité ainsi que la disponibilité des systèmes d'information qui réalise les opérations de gestion nécessaires au maintien en conditions opérationnelles ;

- Le service « Bureautique accueil utilisateurs » a pour périmètre l'innovation et le maintien en condition opérationnelle des outils, logiciels et matériels bureautiques mis à la disposition des utilisateurs ainsi que l'amélioration de l'accueil aux utilisateurs par la mise en place d'un kiosque ;

- Le service « Grands systèmes d'information » qui a pour périmètre la continuité des services et l'évolution des outils logiciels permettant aux agents de la Région d'assurer leurs missions. Ce service élabore, en collaboration avec le métier, les programmes de refonte et de modernisation des SI RH, SI Finances, SI Lycées, SI Achats et la ématérialisation documentaire. Les chefs de projets de ce service sont polyvalents afin d'assurer au mieux la répartition de la charge.

La direction de la donnée rassemble les savoir-faire et compétences autour de la donnée en soutien des pôles qui portent la connaissance métier et assure les missions suivantes :

- Développer et porter la stratégie et la gouvernance de la donnée en interne et vers l'externe, en lien avec les partenaires de la Région. Cette mission vise notamment à assurer la conformité réglementaire, la qualité et la cohérence de la donnée et de ses usages. Elle permet d'appréhender la donnée sur l'ensemble de son cycle de vie, de sa production à sa valorisation ;
- Animer les communautés et écosystèmes régionaux autour de la donnée ;
- Porter une offre d'accompagnement des directions dans l'élaboration et la mise en œuvre de leurs feuilles de route, pour rendre la donnée accessible là où elle peut apporter de la valeur ajoutée et être vectrice d'innovations dans la production des politiques publiques régionales ;
- Développer la culture de la donnée au sein de la Région et auprès de ses publics pour soutenir l'innovation par la sensibilisation, la formation et la mise en place d'expérimentations ;
- Concevoir l'architecture et mettre en œuvre l'outillage permettant à la Région de tirer pleinement partie du potentiel de la donnée. Cet outillage porte à la fois sur les outils et algorithmes (notamment les intelligences artificielles) permettant de transformer, transmettre et valoriser la donnée.
  [Document interne, Région Île de France, 2025]

La direction numérique, innovation et smart rassemble les compétences de gestion et d'appui au déploiement de plates-formes numériques et applicatives. Elle accompagne les grands projets de transformation numérique et d'innovation de la région en s'appuyant sur une expertise centrée sur l'utilisateur.

Elle est composée de trois services :

- Le service « Pilotage des projets de transformation numérique des lycées » qui a pour périmètre la définition et la mise en œuvre du programme stratégique de déploiement du numérique dans les lycées franciliens, le développement, le déploiement, l'exploitation et la maintenance des plates-formes numériques de services au bénéfice

des lycées et de leurs publics, le déploiement, l'exploitation et la maintenance en condition opérationnelle des équipements d'infrastructures réseau et serveurs, des équipements bureautiques de filières et des équipements individuels des élèves et des professeurs, le déploiement sur les plates-formes numériques (ENT, GAR…) des manuels et des ressources éducatives et les développements spécifiques associés ;

- Le service « Grands programmes numériques » a pour périmètre l'amélioration de la qualité de service aux usagers (agents et citoyens) par le développement, la gestion ou l'appui au déploiement de plates-formes numériques de services agrégeant des données et informations internes et externes. Elle accompagne les directions pour définir leurs stratégies numériques d'interaction usagers. Elle anime la communauté interne des chefs de projets et produits numériques. Elle déploie la relation « unifiée » aux usagers ;

- Le service « Connaissance, design et grands projets d'innovation » a pour périmètre la structuration et le pilotage des grands projets d'innovation en se centrant sur la gestion de la connaissance, l'usager et le design. Elle coordonne les réponses transverses associant les différents pôles de la Région aux appels à projets nationaux et européens dans les thématiques de l'innovation en service au territoire. Elle développe un centre de gestion de la connaissance basé sur les compétences de documentation au service des pôles puis du territoire. Elle structure une politique d'innovation par le design et par l'usage.

  [Document interne, Région Île de France, 2025]

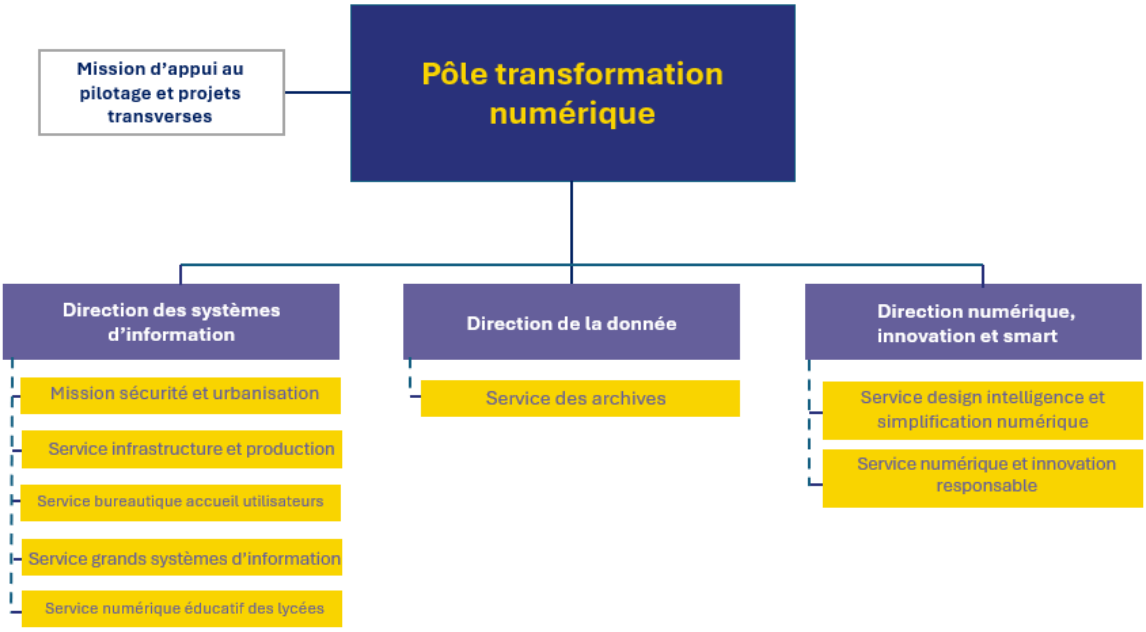

Figure 3 : Organigramme Pôle Transformation Numérique (îledefrance.fr, 2025)

1.2.3. Bureau projet et importance de la transversalité

Dans ce cadre de transformation numérique, de plus en plus de projets complexes sont lancés. Nous pouvons retrouver des portails à destination des franciliens, des interfaces numériques ou encore des outils digitalisés.

Pour accompagner cette dynamique, l'objectif a donc été de centraliser toutes les expertises techniques en un seul pôle, lui-même organisé en trois directions.

L'enjeu de cette réorganisation était ainsi de regrouper des expertises variées et favoriser la transversalité. Malgré les efforts mis en place pour assurer la collaboration, ces équipes restent, à mon sens, encore aujourd'hui trop autonomes et fonctionnent toujours en silos.

Dans ces projets, mon rôle est donc d'assurer un support transverse. Je me situe dans l'équipe « Mission d'appui au pilotage et projets transverses ». Mes missions s'articulent autour de la

coordination des parties prenantes et la facilitation des coopérations entre les différentes directions concernées.

Concretement lorsqu'un projet est initié, les équipes métiers sollicitent des expertises spécifiques : par exemple dans le cadre du RGPD, une équipe métier va solliciter les expertises auprès de la direction de la donnée, mais le projet requierera également des expertises en accessibilité au sein de la direction SMART.

Ma mission consiste alors à articuler les différentes exigences et à les intégrer de façon cohérente au sein du Pôle Transformation Numérique. Je travaille également en lien direct avec les équipes techniques, auprès desquelles je recueille les préconisations qui sont ensuite transmises aux chefs de projets pour orienter les décisions.

Ainsi, mon rôle est d'assurer la coordination et la bonne éxecution de la feuille de route des projets et veiller à ce que l'ensemble des contraintes réglementaires soit prises en compte de manière coordonnée et alignée. En cas de risques, mon rôle est de remonter celui-ci auprès des équipes Projet afin que les équipes modulent leurs actions pour le voir disparaitre, soit auprès d'un Comité qui a le rôle d'arbitrer.

1.3. Court contexte de la cybersécurité

Avant d'entamer la revue de littérature à propos de la cybersécurité il faut comprendre son importance et sa structure au sein des organisations et comment celle-ci fonctionne.

La cybersécurité repose sur une organisation hiérarchisée d'exigences qui vont du stratégique à l'opérationnel. Chaque niveau contribue à la construction d'un dispositif global pour la protection des systèmes d'information. Ces niveaux peuvent être représentés par une pyramide qui offre une lecture claire de la manière dont la cybersécurité se constitue.

1.3.1. Constitution de la Cybersécurité : L'architecture pyramidale

Figure 4 : Cyber Security architecture (David Lineman,2023)

Nous observons sur ce schéma ci-dessus que la cybersécurité peut être représentée sous forme pyramidale divisée en 4 parties.

Au sommet nous retrouvons les Framework de la cybersécurité. Ils représentent les cadres de référence globaux qui orientent la gouvernance de la cybersécurité. Le but de ces Framework est de fournir une méthodologie structurée pour aligner les politiques de sécurité sur les objectifs stratégiques des organisations. Parmi les plus connus et utilisés nous retrouvons ISO/IEC 27000, NIST 800-53, COBIT ou encore PCI DSS. Ces Framework permettent aux organisations de renforcer la résilience et leur maturité en cybersécurité.

Nous allons expliquer rapidement l'interet de ces frameworks :

- ISO/IEC 27000 est une norme internationale qui vient définir les exigences relatives au système de management de la sécurité de l'information. Il s'agit d'une approche par les risques et défend l'amélioration continue.
- NIST 800-53 aux Etats-Unis est un catalogue de contrôles de sécurité et de confidentialité qui couvre de nombreux aspects tels que la gouvernance et la gestion technique.
- COBIT (Control Objectives for Information and related Technology) est un cadre basé sur la gouvernance et le pilotage des systèmes d'information qui intègre la sécurité dans un but de performance et de conformité.

- PCI DSS (Payment Card Industry Data Security Standard) est un framework applicable aux organisations traitant des paiements électroniques permettant de garantir un haut niveau de protection de ces transactions financières.

Le troisième niveau correspond aux politiques de sécurité (politiques de sécurité des systèmes d'information). Elles définissent l'orientation générale et les règles internes d'une organisation. Ces politiques vont encadrer les domaines tels que les contrôles d'accès, la sécurité physique ou l'usage des équipements. Elles sont propres à chaque organisation et traduisent leur volonté en matière de cybersécurité. C'est un référentiel pour l'ensemble des acteurs internes. L'objectif est de faire appliquer cette politique à l'ensemble des employés afin de réduire les comportements à risque.

L'avant dernier niveau regroupe les standards. Ils définissent les règles et normes de référence qui sont applicables dans une organisation. Ils garantissent que les procédures techniques respectent le niveau de sécurité reconnu.

Voici quelques exemples de standards à respecter au sein des organisations :

- Le chiffrement et la protection des données sont soutenus par des algorythmes reconnus par les standards internationaux. Pour le chiffrement symétrique[1] nous retrouvons AES-256[2]. Pour les protocoles de sécurisation des échanges nous pouvons retrouver VPN IPSec[3] pour les connexions distantes.
- L'authentification et les gestion des identités nécéssite souvent l'utilisation de l'authentification multifactorielle qui est notamment exigée dans de nombreux cadres.

La base de la pyramide est donc constituée des procédures opérationnelles et des contrôles techniques qui constituent la première ligne face aux attaques. C'est le point faible de la sécurité. Ce sont les actions concrètes pour prévenir et répondre aux incidents. Ces élements traduisent la sécurité de manière tangible, assurée quotidiennement par les équipes techniques et les utilisateurs.

[1] *Méthode de chiffrement qui utilise une seule clé pour chiffrer et déchiffrer les données*
[2] *Standard de Chiffrement Avancé*
[3] *Logiciel VPN qui utilise le protocole IPSec pour créer des tunnels chiffrés sur Internet.*

1.4. Motivations du mémoire

A l'instar de nombreuses organisations publiques comme privées , le Conseil régional d'Île-de-France a intensifié sa transformation numérique au cours des dernières années. Ces changements s'inscrivent dans l'optique de répondre aux besoin d'efficacité, de modernisation et de proximité avec les usagers franciliens.

La création du Pôle transformation numérique s'inscrit dans cette volonté de strucutrer et professionnaliser les gestion des projets numériques. Intégrée dans ce pôle, les missions sont d'initiatives variées : dématérialisation des services usagers, modernisation des infrastrcutures ou encore développement des plateformes ainsi que la simplification des processus
Cependant cette dynamique de numérisation s'accompagne de constats préoccupants : la cybersécurité bien qu'identifiée comme essentielle et largement valorisée par les dirigeants, demeurent en réalité insuffisamment intégrée dans les pratiques de gestion de projet.
Lors de mes missions j'ai pu observer des chefs de projets fréquemment démunis face à des exigences de sécurité et aux procédures nécéssaires pour les intégrer.
La Région étant composée d'un seul RSSI, ainsi que de son adjoint établi sur la périmètre des actions lycées, pour tout le conseil, l'accompagnement en cybersécurité est encore trop faible. En effet le suivi et la formation restent présents mais de manière trop macro ce qui ne permet pas une réelle intégration du risque.
Les chefs de projets sont ainsi contraints de s'y repérer par eux-même pour intégrer les exigences de sécurités nécéssaires au projet, celle-ci étant trop peu assimilées dans leur processus de gestion de projet.

Ce constat observé au sein de mon organisation relève en réalité d'un constat plus global dans les collectivités françaises. Parmis les principaux freins à l'atteinte d'un bon niveau de sécurité numérique, 47% évoquent le manque de connaissance sur le sujet, 36% le manque de compétence et 36% le manque de budget. Dans ce contexte, les attentes sont claires : 62% des collectivités appellent à une sensibilisation accrue des élus et des agents, 54% à la mise en place d'outils de sécurisation et 45% demandent un accompagnement financier.
L'objectif serait ainsi de renforcer la résilience des collectivités face aux menaces numériques en aidant les équipes à se sécuriser en amont et non dans l'urgence.

Ce constat soulève donc une problématique centrale : comment permettre aux équipes métiers et aux chefs de projet de mieux comprendre, prioriser et intégrer les exigences de cybersécurité dans leurs projets ?

1.5. Diagnostic observé

Afin d'illustrer les problèmes observés lors de cette année d'alternance, j'ai réalisé un diagramme de cause à effet appelé diagramme d'ishikawa représentant les causes d'une cybersécurité fragmentée et peu adaptée au terrain. Le diagramme d'Ishikawa est un outil de gestion visant à identifier et représenter les causes d'un problème spécifique afin de déterminer les origines profondes. Cette analyse se base sur l'étude des 5 M : Mains d'œuvre, Méthode, Matière, Milieu, Matériel.

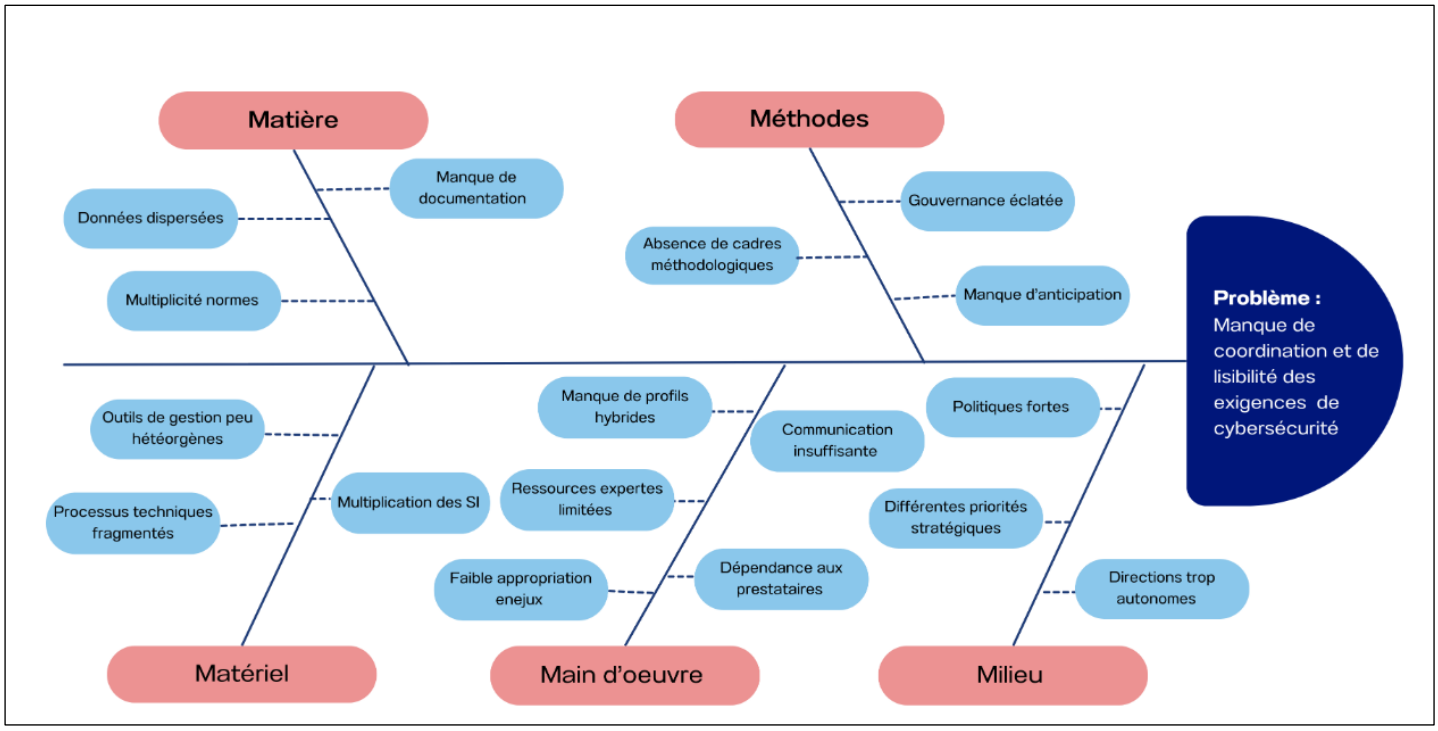

Figure 5 : Diagramme de causes à effets (Personnel)

Matière : Dans les causes liées à la matière nous retrouvons un problème de données. En effet les données sont encore dispersées entre chaque direction qui travaille avec ses propres référentiels. Les qualités peuvent alors varier et être mal structurées. Le manque de documentation rend ainsi leur réutilisation difficile.

Dans un second temps, la transformation numérique fait face à une multiplicité d'exigences réglementaires et normatives. Elles concernent notamment le RGPD, l'accessibilité numérique, l'open Data et bien sur la cybersécurité.
A cela s'ajoute des cahiers des charges parfois incomplets ou trop généraux. Les équipes peuvent faire face à un manque de cartographie claire des exigences, d'autant plus que certains livrables produits par les directions sont peu harmonisés et difficilement exploitables.
Et enfin il est certain que le Pôle manque d'outils centralisés pour suivre l'évolution des contraintes et souffre d'une absence de tracabilité pour la gouvernance des exigences.

Méthodes : La Pôle fait face à l'absence d'un cadre méthodologique commun. En effet chaque direction applique toujours ses propres méthodes (agile, cycle en V..) ce qui génère des décalages. De plus, il n'existe pas de référentiel clair de gestion de projet unifié intégrant les contraintes transverses. Le seul outils existant un un excel complexe parcouru de question illisibles pour les chefs de projet. Il est alors difficile de prioriser les exigences.
Cela induit une intégration tardive des exigences transverses. Les exigences telles que la cybersécurité ou l'accessibilité sont souvent considérées après coup au lieu d'etre intégrées dès la conception. Les exigences essentielles sont également traitées en silos, sans articulation fluide dans le projet.
La gouvernance apparait fragmentée par la multiplicité des interlocuteurs. Un manque de clarté sur les arbitrages rend les instances de pilotage irrégulières et complexes.
Le suivi des projets manque d'indicateurs définis et partagés entre les directions, il est alors difficile de mesurer la conformité aux différentes exigences. Et enfin la communication et la coordination non formalisées ne permettent pas une bonne fluidité de l'information entre les équipes.

Matériel : Malgré la volonté d'unifier les trois directions celles-ci gardent leur mode de fonctionnement et utilisent leurs propres outils (excel, jira…) sans mise en commun. Il est alors difficile de centraliser les informations dans une plateforme commune. De plus une multiplication des canaux de suivi rend le risque de perte d'information plus importante.
La dépendance aux prestataires externes est très forte cela implique une maintenance externalisée qui provoque de plus grandes lenteurs pour corriger les problèmes.

Main d'œuvre : Le conseil régional se heurte à des compétences internes limitées. Peu de profils hybrides sont instaurés pour comprendre à la fois les enjeux métiers, techniques et

réglementaires. De plus les experts sont en nombre trop restreint. Il y a alors une surcharge de travail et un goulot d'étranglement qui induit des risques d'exigences oubliées, de projets passés trop rapidement et d'accompagnement insuffisant.
Certaines contraintes sont perçues comme externes plutôt que comme des leviers de qualité, les dimensions réglementaires ne sont alors pas suffisament intégrées dès la phase de conception.
La sensibilisation et la formation, qui sont des instruments stratégique pour les enjeux de sécurité sont organisés par les référents dans le but d'établir une culture du risque. Toutefois, malgré ces initiatives, l'assimilation par les agents demeure limitée. D'autre part le langage des experts est parfois difficilement traductible et compris par les chefs de projet. Le fort Turn-Over au sein des équipes de la région constitue un frein majeur à l'acculturation aux risques. En effet cela limite la continuité des apprentissages et accentue les difficultés de compréhension de langage de la sécurité. Le risque de malentendus est accru et intensifie le risque de perte d'informations.
Et enfin, la région fait appel à de nombreux prestataires externes pour certaines expertises clés. Le manque de transfert de compétences vers les équipes internes induit un risque de dépendance prolongée et empeche l'appropriation des enjeux par les agents.

Milieu : L'oganisation en silos persiste malgré des volontés de rendre la collectivité plus agile. Malgré la création du pôle unique, les anciennes habitudes demeurent et la resistance au changement est forte chez les agents.
Au sein d'une organisation avec de forts enjeux et en charge d'obligations fortes envers les franciliens, l'environnement réglementaire et politique est très complexe. Les normes à respecter se multiplient et la pression est forte de la part des instances de contrôle et des obligations légales. Les décisions influencées par des enjeux politiques ou d'image sont nombreuses. Les projets numériques sont réalisés dans un environnement public avec des lourdeurs administratives sur les délais ou les arbitrages. Certaines priorités stratégiques sont divergentes entre directions métiers, données et techniques.
Et enfin la culture organisationnelle peine à être instaurée laissant la cybersécurité perçue comme un sujet trop « technique ».

2. *Problématique retenue*

Ce diagnostic des dysfonctionnements observés permet de retenir une problématique.
En effet la transformation numérique des collectivités s'accompagne de la montée en flèche des exigences en matière de cybersécurité. Les risques cyber ayant fortement augmentés, les organisations se voient forcées de mettre en place des mesures de manière plus rapides et plus fortes non nécéssaires auparavant. Autrefois considérée comme une responsabilité uniquement technique relevant des experts, elle s'impose aujourd'hui comme un enjeu transversal qui concerne l'ensemble des acteurs d'une organisation impliqués dans quelques projets numériques. Malgré son importance cruciale, son intégration dans les projets reste complexe.
En effet les chefs de projets sont soumis à une double difficulté, la navigation dans un environnement marqué par une densité réglementaire en parallèle d'une traduction opérationnelle floue et fragmentée. Par ailleurs, ils doivent évoluer au sein d'une gouvernance interne éclatée ou les responsabilités en terme de sécurité sont parfois peu définies entre directions métiers, DSI et les instances de contrôle.
Cette situation peut engendrer plusieurs conséquences telles que l'intégration tardive des exigences de cybersécurité au cours des projets ou encore une collaboration désorganisée entre les chefs de projet et les experts techniques. Cela infflue sur les risques de non-conformité et de vulnérabilités. Ces perspectives mettent en lumière un certain paradoxe : si la cybersécurité est aujourd'hui reconnue comme un enjeu stratégique majeur, sa mise en œuvre concrète au sein des projets numériques reste illisible pour les acteurs non spécialisés.

C'est dans ce contexte que j'ai retenue la problématique suivante : ***Comment piloter efficacement les exigences de cybersécurité dans un contexte organisationnel marqué par un manque de clarté, la fragmentation ou l'absence de procédure structurée ?***

PARTIE 2 – REVUE DE LITTERATURE

La revue de littérature présentée prochainement a pour objectif d'ancrer mon mémoire dans la littérature et les travaux existants afin d'éclairer la problématique retenue par des analyses de recherches et des cadres théoriques existants. Cela va nous permettre d'identifier les exigences qui structurent la gestion des projets numériques ainsi que les apports et les limites des approches actuelles de la cybersécurité. En articulant ces différentes contributions, nous pourrons mettre en évidence les tensions, les zones d'illisibilité ainsi que les perspectives qui justifient cette démarche de recherche.

1. Transformation numérique et nouvelles exigences dans les organisations

1.1. Piloter les exigences

Les sociétés contemporaines traversent de profondes mutations qui remodèlent simultanément nos structures économiques et sociales ainsi que nos dynamiques professionnelles. Le monde du travail, en particulier, se trouve au cœur de ces transformations, marqué par des évolutions rapides largement portées par le développement des technologies numériques.

Ces transformations évoquées ne se traduisent pas uniquement par l'automatisation des taches et des processus ou par la multiplication des supports numériques. Elles viennent également transformer les formes d'organisation, les temporalités du travail et l'expérience subjective du travail en lui-même. Il est désormais bien évident que les technologies ont reconfigurées notre façon de travailler et bouleversées de nombreuses professions. Pourtant, ce fait cache un bouleversement plus profond impliquant les dynamiques économiques, politiques et culturelles. Comme l'explique [Doray, 1992], les professions ne peuvent plus être définies uniquement par des taches techniques, elles sont façonnées par un ensemble complexe de normes implicites, de savoir faires tacites et de relations sociales qui construisent l'identité professionnelle.

1.2. Les projets numériques

[Lepage, 2021] traduit la transition numérique telle une grappe d'innovations technologiques marquée principalement par le développement massif de l'informatique. Ceci débute dans les années 30 puis est accompagné du développement web au début des années 1990. Cette transition numérique découle d'un processus évolutif continu qui se poursuivra encore durant de nombreuses années.

Il est cependant essentiel de distinguer « transition numérique » et « transformation numérique » comme le soulignent [Hilary et al, 2024]. En effet la première décrit l'adoption progressive des technologies permettant d'améliorer les processus existants d'une entreprise. Ces innovations ont ainsi permis le traitement de texte pour produire des textes de manière plus efficace. Ou encore l'apparition du courriel pour diffuser les textes. Ces innovations font désormais parties intégrantes des routines en entreprise mais n'ont pas fondamentalement bouleversées les modes de fonctionnement.

A contrario la transformation numérique à induit un changement profond dans les manières d'opérer. La transition numérique se concentre sur l'intégration graduelle de technologies qui permettent l'amélioration de l'efficacité opérationnelle. [Birnbaum et al., 2005] affirme alors que la transformation numérique est quant à elle disruptive. Elle entraine ainsi une transformation totale de nos processus et de nos modèles d'affaire. C'est dans ce contexte de transformation que les projets numériques prennent formes.

Henri Kloetzer donne une définition claire d'un projet informatique : « *Un projet informatique existe d'abord conceptuellement, par ses objectifs, sa cible, ses délais et son budget. [...] un projet informatique est un investissement, destiné à contribuer aux objectifs de l'entreprise.* » [Kloetzer, 2015] Il ajoute par la suite qu'un projet informatique varie en termes d'échelle et de niveau de complexité et peut naturellement concerner des individus, des équipes ou des organisations différentes. Les projets numériques incluent généralement la création d'une application, l'analyse de données, le développement d'un système ou encore la création d'un service ou d'une plateforme numérique.

1.3. Les exigences dans les projets numériques

Le glossaire CFTL/REQB des termes utilisés en ingénierie des exigences définit une exigence comme *« une condition ou capacité requise par un utilisateur pour résoudre un problème ou atteindre un objectif qui doit être tenu ou possédé par un système ou composant pour satisfaire à un contrat, standard, spécification ou autre document imposé formellement »* [CFTL, 2011 d'après IEEE 610]. C'est donc l'ensemble des besoins, attentes ou encore contraintes qu'un produit ou système doit satisfaire.

Ces exigences sont au cœur du pilotage des projets et constituent le point de départ de chaque projet par leurs planifications et leurs conceptions.

L'exigence correspond ainsi à une finalité de satisfaction énoncée clairement : « un énoncé qui prescrit une fonction, une aptitude ou une caractéristique à laquelle doit satisfaire un produit ou un système dans un contexte donné » [Bourey et al., 2010]. La gestion des exigences est donc une activité non négligeable et centrale de l'analyse métier. Le [SWEBOK, 2014] complète cette définition par : « *A requirement is defined as a property that must be exhibited in order to solve some problem of the real world*. » Elle comprend plusieurs volets tels que la planification, le suivi, l'analyse ou encore la communication et la gestion. Ces exigences aboutissent généralement à un Plan de Gestion des Exigences et se concrétise dans les projets d'envergures comme des documents formels et plans spécifiques. L'objectif principal d'une exigence est ainsi d'assurer la compréhension approfondie des besoins métiers et implique ainsi une élaboration progressive du niveau global vers des niveaux plus détaillés. [Larson et al., 2008 ; Wanderley et al., 2014]

Une exigence doit être claire et détaillée pour rassurer les utilisateurs sur la couverture de leurs besoins. Mais elle doit également être exploitable par les équipes de développement afin de concevoir le produit ou service attendu.

1.3.1. Typologies d'exigences

Les exigences peuvent couvrir des formes variées et répondre à des finalités distinctes. Parmi elles, figurent les exigences fonctionnelles, qui définissent les actions que le système doit opérer en fonction des besoins exprimés par les utilisateurs

Nous retrouvons par la suite les exigences non fonctionnelles qui correspondent au critère du fonctionnement, « comment le système fait ». Ces exigences prescrivent donc les processus à suivre et les contraintes de réalisation du système.
Les exigences réglementaires sont-elles traduites par les normes légales à respecter telles que le RGPD, l'accessibilité numérique… elles sont ainsi édictées par les autorités nationales et européennes et complétées par un ensemble de recommandations pratiques et de textes normatifs encadrés par des autorités nationales tel que la CNIL ou l'ANSSI.
Les exigences organisationnelles rassemblent les contraintes de déploiement, de gouvernance ou encore de formation… elles nécessitent une coordination de ressources permettant d'organiser une action et de parvenir à l'accomplissement de cette même action. [Indeed, 2024]

Ces typologies d'exigences sont toutes mises en place pour répondre à des fonctions claires : aligner les parties prenantes autour d'un objectif commun, réduire les ambigüités dans la réalisation des projets, faciliter les contractualisations, prévoir les ressources nécessaires et enfin encadrer les phases de test, de validation et de recette.
Les exigences servent en fin de compte à guider ce à quoi doit répondre le projet tout au long de son cycle de vie. [Larson et al., 2008]

1.3.1.1.Les exigences spécifiques aux collectivités

Les collectivités territoriales restent cependant plus confrontées a des exigences plus denses que celles du secteur privé. En effet celles-ci sont également soumises aux obligations telles que l'open data qui impose la publication et la diffusion des informations publiques selon un objectif de transparence et d'accessibilité citoyenne. De plus, elles doivent respecter des règles strictes d'archivage. La conservation ainsi que la traçabilité et la sécurisation des documents administratifs sont encadrés par un cadre légal exigent. [Perrin, 2021] Celui-ci est également assorti de durées de conservation plus longues que dans les entreprises privées.
D'autres contraintes majeures viennent s'ajouter telles que l'accessibilité numérique. Les collectivités sont obligées de de suivre des règles de conception des services et d'applications inclusives pour tous les usagers et en particulier les personnes en situation de handicap en suivant le RGAA (Référentiel général d'amélioration de l'accessibilité). De nombreuses communes françaises font face à un retard en termes d'accessibilité [Devilliers, 2025]. L'urbanisation des systèmes d'information vise également à assurer la cohérence et l'interopérabilité des nombreux outils déployés au sein des services publics. Enfin les

contraintes liées au budget publics impliquent de concilier rigueur financière, arbitrage politique et priorisation des projets. Les exigences renforcées de la sécurité réseau conditionne la protection des infrastructures critique ainsi que la continuité des services publics.

Toutes ces obligations accumulées viennent ajouter une charge accrue pour les chefs de projet. Il y a d'avantages de normes à appliquer, plus de mesures techniques et organisationnelles à prendre ainsi qu'une multiplicité d'interlocuteurs à confronter. Cette multiplicité explique en partie la complexité de la gestion de projet dans les collectivités ou la réussite dépend de nombreux facteurs dans un cadre légal et organisationnel contraint.

1.3.2. Ingénierie des exigences

« L'ingénierie des exigences est reconnue comme un processus social qui se caractérise par des prises de décisions permanentes entre de nombreux participants (gestionnaires, utilisateurs finaux, et analystes du système) »[Wanderley et al., 2014]
L'ingénierie des exigences désigne donc l'ensemble des activités qui permettent d'identifier, d'analyser et gérer les exigences exprimées par les différentes parties prenantes d'un projet. Cette discipline prend une place à part entière dans la gestion de projet et est particulièrement nécessaire dans un contexte de projets numériques ou les systèmes sont complexes et les attentes et risques élevés. Elle est bien entendue commune à toutes les ingénieries métiers car reconnue comme la phase la plus décisive en amont de tout projet.[Bourey et al., 2010]

Selon la norme ISO/IEC/IEEE 29148, l'ingénierie des exigences englobe quatre grandes phases en amont du projet :

- L'élicitation des besoins et services énoncés par les utilisateurs finaux.
- L'analyse des exigences qui implique la cohérence, la faisabilité et les conflits.
- La spécification qui désigne la rédaction formelle et des exigences énoncées.
- La vérification/ validation des exigences avec les utilisateurs finaux.

Une bonne ingénierie des exigences doit permettre de réduire les défauts le plus tôt possible et de clarifier en aval les objectifs métiers et acteurs nécessaires. L'objectif est d'améliorer la qualité des exigences en atténuant les défauts, omissions ou erreurs souvent rencontrés dans la phase d'expression des besoins et inhérents à la nature informelle de ces derniers. [Bourey et

al., 2010]. Une ingénierie mal conduite est une cause très fréquente d'échecs de projets. Le Software Engineering Institute estime à près de 60% des défauts projets découlent d'une mauvaise traduction des exigences.

Dans un environnement marqué par une complexité réglementaire, l'ingénierie des exigences n'est plus une option. Celle-ci doit être considérée comme une étape nécessaire et cruciale intégrée comme levier stratégique de gouvernance. [Bourey et al., 2010] Elle est notamment essentielle pour l'intégration des exigences transversales telles que la cybersécurité, l'accessibilité ou encore l'open data.

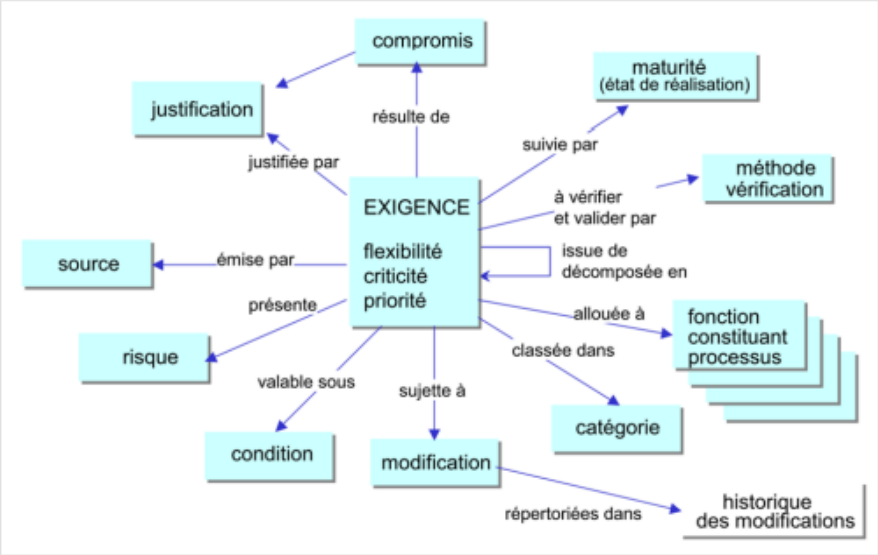

Figure 6 : Modèle de données des exigences (AFIS.)

Ce modèle de données des exigences illustre la manière dont les différentes exigences sont structurées et interdépendantes dans un projet. Cela met en évidence les relations entre les besoins métiers, les exigences fonctionnelles et non-fonctionnelles et les contraintes. Nous pouvons observer la complexité de ces exigences qui souligne l'utilité d'une ingénierie rigoureuse pour éviter les incohérences et les oublis. Ce type de modèle est un support utile à l'analyse et à la traçabilité des exigences lors du cycle de vie d'un projet.

1.4. Les projets numériques comme vecteurs de transformation

1.4.1. Evolution du métier de chef de projet : nouvel acteur du changement

Le chef de projet a toujours joué un rôle central dans l'orchestration des différentes dimensions d'un projet, que ce soit le déroulé du projet, le budget, le calendrier ou encore la coordination entre les différentes parties prenantes.

Mais dans un contexte numérique, ce rôle devient de plus en plus complexe.

Dans son article intitulé : « Digital Skills for Project Managers: A Systematic Literature Review »,[Marhraoui, 2023] souligne que les compétences numériques sont devenus aussi importantes que les compétences techniques classiques et les connaissances interpersonnelles. En effet le chef de projet doit être multitâche et s'adapter parfaitement aux nouveaux outils. Il doit pouvoir piloter des équipes à distance, intégrer des outils collaboratifs mais avant tout anticiper les impacts des technologies sur la structure même des projets. Cela implique d'intégrer toutes les dimensions réglementaires liées aux projets numériques.

[Marhraoui, 2023] démontre donc le rôle élargit du chef de projet et notamment dans le contexte numérique. Désormais les chefs de projet doivent alterner entre compétence numériques avancées, visions stratégiques des enjeux numériques et notamment des risques cyber (RGPD, cybersécurité…). Viennent s'ajouter les compétences de leadership et leur capacité à évoluer dans un monde bien incertain. Le chef de projet n'est plus un simple exécutant mais désormais un stratège et facilitateur aux premier plan des projets.

Par ailleurs, le chef de projet devient un agent de transformation portant une vision et un accompagnement face aux rupture stratégiques. [Animashaun et al., 2024] évoquent le repositionnement du chef de projet tel un stratège de la transformation numérique et notamment dans le secteur public. Cela s'explique par son rôle clé dans la conduite du changement mais de manière très importante dans la coordination des acteurs multiples. Ils expliquent ainsi : « *La gestion stratégique de projet joue un rôle crucial dans la réussite de ces transformations. Elle fournit une approche structurée permettant de superviser et d'orienter les projets de transformation numérique, tout en aidant les organisations à maximiser leur impact et leur efficacité, en gérant les risques et les ressources de manière optimale.* » Les auteurs viennent appuyer cet argument par le besoin de maitriser les outils de gestion mais aussi de comprendre l'impact organisationnel des technologies telles que le cloud, l'IA et l'automatisation. Ces compétences sont essentielles pour participer aux arbitrages technico-politiques, il devient ainsi garant de la création de valeur continue.

1.4.2. La complexité accrue des environnements numériques

Cette numérisation des outils engendre une certaine complexité face à la mise en place d'un projet. Désormais les projets numériques reposent sur des architecture technologiques complexes prenant en compte les API[4], le cloud en encore l'interopérabilité. Cela rend l'analyse plus critique.[Ochoa Pacheco et al., 2023; Animashaun et al., 2024]. Cette complexité s'accompagne d'une multiplication des exigences qu'elles soient techniques, légales ou éthiques. Cela impose une surcouche de pilotage réglementaire et de logiques de conformité que les chefs de projet doivent intégrer dans des délais opérationnels contraints. [Lepage, 2021] [Marhraoui, 2023] ajoute à cela que le chef de projet doit comprendre les dépendances entre les briques technologiques sans forcément y être un expert. Cependant cette complexité accrue engendre un risque de défaillances systémiques et de chevauchements entre les projets qui vont amplifier les incertitudes.

Viennent s'ajouter les contraintes de délais pouvant être imposés par une volonté politique. Il demeure une désynchronisation entre l'innovation et les processus institutionnels. Des tensions tendent à naitre face à des délais très courts pour la production mais des attentes très longues pour les validations.

Le chef de projet n'est donc plus seulement responsable d'un périmètre technique restreint, mais d'un système sociotechnique ouvert en perpétuel évolution. [Szpitter et al, 2016] expriment ce phénomène par la méthode VUCA[5]. Pour eux désormais l'environnement projet est volatile, incertain, complexe et ambigu.

Le concept VUCA est proposé par la première fois par l'United States Army War College dans le but de décrire et analyser la volatilité, l'incertitude, la complexité et l'ambiguïté de situations ou de conditions données.[Canzittu, 2022] Ce modèle illustre un monde actuel sujets aux évolutions et transformations constantes qui nécessite une remise en question perpétuelle de la part des organisations pour survivre aux aléas de l'environnement.

[4] *API = interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités*
[5] *Méthode VUCA : Volatility, Uncertainty, Complexity and Ambiguity*

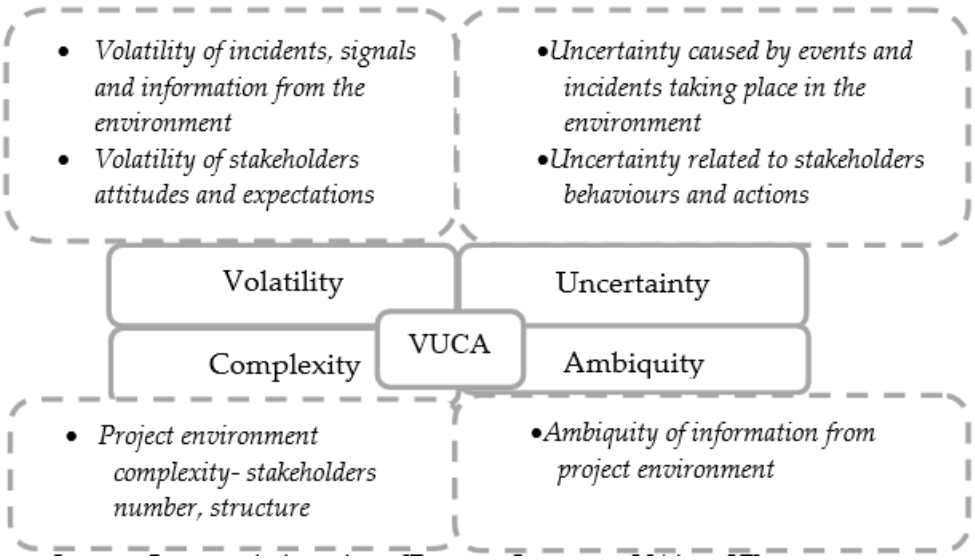

Figure 7: envrionnement VUCA (Bennett, Lemoine, 2014, p. 27)

Dans cet environnement complexe s'ajoute la pression temporelle et organisationnelle constante. Les attentes sont fortes concernant la livraison rapide, la réduction des couts mais aussi l'expérimentation rapide. Le chef de projet doit ainsi gérer des contradictions entre la qualité, la rapidité et la robustesse du produit.[Brill et al., 2006] Cette contradiction est notamment formalisée par [Clegg et al.,2018]. [Kerzner, 2004] parle de « triple constraints » : Cost, time, scope. Les chefs de projet vont donc devoir effectuer un arbitrage pour ainsi prioriser les risques.

Figure 8 : The triple constraint (Harold Kerzner, 2004)

Ce schéma du « triple constraint » illustre l'équilibre entre les trois dimensions fondamentales d'un projet : le coût, le délai et le périmètre. Chaque modification d'un des trois paramètres affecte directement les deux autres.

Cette priorisation s'explique également par la multiplication des projets en simultané dans les organisations. Ces portefeuilles de transformation numériques surchargent les ressources humaines et les équipes techniques. Cela implique que les chefs de projet doivent souvent composer avec des équipes partagées et peu disponibles. [Lepage, 2021]
Pour finir les nouveaux environnements agiles peuvent créer une certaine complexité de par leur itérations permanentes ou encore les priorisations évolutives. Le pilotage doit donc intégrer la flexibilité sans le sacrificie de la cohérence d'ensemble.

1.4.3. Les nouvelles logiques de pilotage

1.4.3.1.Transversalité accrue et gouvernance fragmentée

Les projets numériques incluent une gouvernance élargie et une transversalité accrue. En effet ils impliquent une multiplicité d'acteurs face aux différentes obligations tels que la DSI, les directions métiers, les aspects juridiques mais encore les prestataires ou les usagers. La gouvernance devient donc transversale. Selon [Clegg et al., 2018] cette configuration impose aux chefs de projet de développer une capacité à aligner les logiques, parfois divergentes, des différentes parties prenantes.
Cette observation est particulièrement présente dans le secteur public. En effet, face à ces configurations, le chef de projet public est contraint de composer avec une gouvernance distribuée et même parfois fragmentée[Pisa et al, 2013] Ce constat est renforcé par [Animashaun et al., 2024] qui appuient que désormais la gouvernance projet s'oriente vers des modèles plus distribués et partagés ou le pouvoir décisionnel est décentralisé. Particulièrement dans les projets publics, les chefs de projets doivent aligner les priorités politiques, techniques et citoyennes.

1.4.3.2.L'adoption des méthodes agiles

Les organisations ont désormais recours aux méthodes agiles (Scrum, Kanban, SAFe…). Ces nouveaux outils s'imposent dans de nombreux projets numériques et particulièrement quand ceux-ci sont incertains ou risqués. Ils modifient donc la posture classique du chef de projet autrefois basée sur un déroulement séquentiel. Celui-ci passe de gestionnaire à celui qui facilite l'organisation collective du travail. Le chef de projet doit désormais apprendre à partager le pouvoir. Comme l'expliquent [Müller et al., 2018], le rôle des chefs de projet évolue vers un leadership distribué. Il faut ainsi apprendre à partager le pouvoir, à faciliter plutôt que contrôler mais aussi accepter et évoluer avec l'incertitude comme un élément majeur du projet. La temporalité d'un projet devient ainsi itérative et adaptative. Cela impose des revues fréquentes et des ajustements continus. Désormais la réactivité prime sur la stabilité [Brill et al., 2006]

Le constat est généralement un peu différent dans le secteur public. L'adoption des méthodes agiles se heurtent souvent à des contraintes institutionnelles fortes notamment par le cadre juridique, les cycles budgétaires ou encore la reddition des comptes. Malgré tout, des programmes agiles sont lancés depuis 2024 au sein du Conseil pour tenter de pallier ces écarts.

1.4.3.3.La participation des parties prenantes

Le pilotage des projets modernes inclut désormais les usagers finaux dès la phase de conception. Cela s'inscrit dans une logique de co-construction et de test continu. On y inclut le design thinking, l'UX, l'accessibilité… Cela suppose une redistribution des pouvoirs dans la conduite de projet comme expliqué par [Cicmil et al., 2006] Ils énoncent cette approche comme remettant en cause le pouvoir descendant des experts. De plus, [Ochoa Pacheco et al., 2023] rajoutent que le chef de projet doit porter des démarches collaboratives avec des groupes d'acteurs hétérogènes et la plupart du temps non techniques. Cela nécessite pour lui de bonnes compétences en communication, médiation ou encore facilitation.

Dans le secteur public, la co-construction est valorisée et mise en avant notamment politiquement. Celle-ci renforcerait la légitimité des projets, mais en contrepartie complexifie leur pilotage. [Lepage, 2021]

1.4.3.4.Transition vers un profil hybride

Face à cette transformation des organisations, à la complexité de l'environnement métier et aux nouvelles méthodes de pilotage le rôle même du chef de projet évolue vers un profil

hybride. Les compétences traditionnelles sont redéfinies. En effet, il devient un acteur stratégique à l'intersection de multiples dimensions à la fois humaines, techniques, réglementaire mais aussi politiques dans les collectivités. [Ochoa Pacheco et al., 2023] évoquent trois compétences clés pour les chefs de projets publics : techniques, comportementales et contextuelles. Cette hybridation du profil se traduit par la maitrise des outils et méthodes projet mais parallèlement d'une capacité à comprendre les architectures numériques, les enjeux et l'écosystème des parties prenantes. [Brill et al., 2006] renforcent cette idée en démontrant que la performance d'un chef de projet combine savoir-faire technique, sens politique et compétences relationnelles.

1.4.3.5.Les Soft Skills

Face aux différentes tensions présentes dans le monde du travail, les chefs de projet doivent désormais faire preuve d'aptitude relationnelles fortes pour piloter des équipes pluridisciplinaires. Il maintient de gérer ces tensions et maintenir une cohésion entre les acteurs. Selon l'étude réalisée par [Brill et al., 2006], la communication, l'intelligence émotionnelle et la capacité à motiver les équipes sont devenues les compétences les plus critiques selon les experts.

Face à un environnement projet transversal, le chef de projet doit pouvoir influencer les équipes sans autorité directe. Les « *soft skills* » deviennent indispensable. C'est ainsi que les projets réussis résultent la plupart du temps du pilotage par des chefs de projet capables d'ajuster leur style de leadership selon les personnes et le contexte. Un leadership mobilisateur permettra de faire adhérer les équipes à la vision du projet malgré la résistance au changement présentes dans certaines équipes. Il faut ainsi ajuster son équilibre entre personne et performance pour un meilleur résultat projet. [Müller et al., 2018]

Il faut ajouter aussi la communication claire et structurée comme nécessité dans un contexte d'incertitude. Un chef de projet précis et concis réduira les incompréhensions des acteurs et facilitera leur alignement. [Ochoa Pacheco et al., 2023] Et enfin, levier non négligeable de performance, l'écoute active est essentielle pour une agilité organisationnelle et ajuster la posture du projet.

Face aux arbitrage complexes mentionnées en amont, qui peuvent créer des tensions internes, la médiation et la diplomatie sont des atouts clés.

Ces situations induisent des charges émotionnelles importantes car il faut réussir à la fois à motiver, négocier, rassurer dans des climats incertains. La maturité émotionnelle est alors devenue une compétence clé. [Kerzner, 2004]

1.5. Charge normative

Désormais les chefs de projet numériques sont face à un environnement juridique contraint ou la conformité dépend des directions juridiques ou des RSSI. [Lepage, 2021] explique que dans les collectivités les responsabilités sont diffuses et mal réparties. Cela tend à placer une pression sur les chefs de projet pour sécuriser les projets. En effet, désormais, il faut anticiper les implications juridiques dès la phase de conception des projets tels que la protection des données, les droits d'auteur, l'accessibilité, la commande publique…Cette pression est nécessaire autant qu'elle est contraignante. Les risques juridiques, économiques et éthiques sont importants et fortement médiatisés ces dernières années.

C'est ainsi qu'ils composent avec un empilement d'exigences techniques, juridiques, politiques et éthiques dictées par une certaine poly conformité implicite [Lepage, 2021]. Ceci s'explique par une multiplicité des normes et des obligations à respecter ainsi qu'un manque d'outils de traduction opérationnelle pour aider les chefs de projets dans leur processus.

Dans les collectivités particulièrement, un cadre normatif fort pèse sur les chefs de projet. Ils sont très nombreux et s'imposent dans tous les différents aspects du projet. L'accessibilité, le RGPD, la sécurité, les données, l'urbanisation, le design…sont des entités qui, composées de normes et de concepts encadrés par des règlements, doivent être prises en compte par les chefs de projet. Les projets sont d'autant plus soumis à des temporalités administratives et des politiques spécifiques dans les collectivités. Ils sont souvent porteurs d'une symbolique politique forte.

1.6. Conclusion de la section

Cette première section a permis de clarifier les fondements liés à la gestion des exigences dans les projets numériques. Nous avons pu illustrer dans cette partie les notions de besoins, d'exigences ainsi que leurs relations avec les contraintes organisationnelles et réglementaires. Le rôle était ainsi de comprendre le rôle structurant des exigences dans le pilotage des projets.

2. La Cybersécurité – Panorama d'un risque systémique

La cybersécurité s'impose aujourd'hui comme un enjeu majeur pour les organisations publiques comme privées. Loin de la dimension technique, il est incontournable de la considérer comme une problématique systémique touchant les infrastructures mais aussi les processus de gouvernance et la confiance des usagers. En effet la multiplication des attaques de toutes sortes révèle la vulnérabilité structurelle des systèmes d'information et met en lumière l'ampleur des risques auxquels sont confrontés les organisations. En effet le risque systémique désigne un risque dont les effets dépassent largement la simple échelle d'une organisation isolée mais affecte un ensemble interconnecté d'acteurs, de secteurs mais aussi de l'ensemble d'une société. [Forscey, 2022]

La cybersécurité ne peut plus être vue comme un domaine isolé réservé aux spécialistes techniques. Elle doit être intégrée dans une approche globale de gestion des risques. Dans cette perspective il est nécessaire de dresser un panorama de la cybersécurité comme un risque systémique afin de mieux comprendre les menaces actuelles, leur évolution et les conséquences sur la conduite des projets numériques.

2.1. Emergence de la cybersécurité

« *La question ne sera plus de savoir si une structure sera ou non la cible des attaquants, mais elle est de savoir quand cela arrivera.* » expliquait M. POUPARD, ancien Directeur de l'ANSSI[6] en 2015. La cybersécurité s'est imposée comme une préoccupation majeure à mesure que le numérique a pénétré la société contemporaine. Délaissée par les communautés scientifiques et d'experts en Sécurité, cette notion a pris une place prépondérante à l'échelle mondiale aussi bien dans le monde professionnel que personnel. Cette numérisation de la société a conduit Douville à affirmer : « *Aujourd'hui, tout est numérique, et ce qui ne l'est pas le sera bientôt* » [Douville, 2020]

Dans les années 1980, émergent les premiers virus malveillants. En effet, si la sécurité informatique était auparavant limitée aux mondes militaires et universitaires, les années 80 ont

[6] *Agence nationale de la sécurité des systèmes d'information*

été témoins de la prolifération des premiers virus informatiques et souligne la multiplicité des cibles : données scientifiques, données personnelles. Le fameux épisode du Ver Morris de 1988 a mis en lumière la vulnérabilité des réseaux. Cette vulnérabilité, couplée aux menaces cyber, nous amène à comprendre ces attaques comme des risques à part entière. C'est dans le but de contrer ces nouvelles menaces que les logiciels antivirus ont été développés, marquant ainsi le début de la lutte contre la cybercriminalité.

2.2. Définitions

Pour comprendre la notion complexe de la cybersécurité, il est nécessaire de recourir à des définitions à la fois scientifiques et des définitions juridiques. [Delorme, 2023] « *On peut voir depuis peu une utilisation massive du terme cybersécurité malgré le fait que celui-ci souffre d'un manque de consensus quant à sa définition* »

La cybersécurité est généralement définie comme *« la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données et de services connexes*. » [Douville, 2020]

En ce sens elle désigne la protection des systèmes d'information contre le vol ou les dommages affectant le matériel, les logiciels, ainsi que les données qu'ils contiennent, mais aussi contre toute perturbation ou détournement des services qu'ils fournissent.

[Craigen et al., 2014] définissent quant à eux la cybersécurité comme « *the organization and collection of resources, processes and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights* ».

Ces définitions renvoient en creux à la notion de virus informatique formalisée par Fred dans ces travaux en 1987. Ce dernier a démontré la capacité d'un programme à se reproduire et à infecter d'autres programmes.

La cybersécurité qui est désormais considérée comme un pilier de la sécurité informatique [Schatz et al., 2017] est fondée sur la définition de la cybernétique de Norbert Wiener [Wiener, 1948]. Elle est aujourd'hui essentielle et sujet d'actualité pour de nombreuses entreprises, gouvernements et individus.

[Karabacak et al.,2016] apporte certaines précisions quant à la notion de cybersécurité. Cette notion repose sur des pratiques organisées qui impliquent à la fois des dimensions techniques mais également sociales. La cybersécurité est essentielle pour protéger les systèmes

d'information mais aussi les systèmes numériques dans leur ensemble. En effet elle dépasse la simple protection des données, elle est désormais perçue comme une question de souveraineté.

2.2.1. Les 3 piliers de la cybersécurité

La cybersécurité repose sur 3 principes fondateurs clés qui constitue le socle inébranlable de toute politique de sécurité. Connus sous le nom de triangle de CID, c'est un acronyme qui représente les trois principes essentiels : protéger les données (confidentialité), s'assurer qu'elles soient exactes (intégrité) et s'assurer qu'elles sont disponibles quand nécessaires (disponibilité). [Delorme, 2023]

La confidentialité signifie la préservation du caractère privé ou secret de l'information. Il garantit l'accès aux données uniquement aux personnes habilitées. Cet aspect est essentiel dans les organisations possédant des données personnelles ou sensibles. Il est généralement garanti par les méthodes de contrôles d'accès ou de chiffrement.

L'intégrité fait référence à la précision et à la cohérence des données lors de leur cycle de vie. C'est une assurance sur la qualité et fiabilité des données pour prévenir les violations ou la corruption de données.

Pour finir, la disponibilité fait référence au fait de s'assurer que les informations et les ressources sont uniquement accessibles aux utilisateurs habilités en cas de nécessité.

Cette notion s'avère indispensable pour maintenir la continuité de l'activité et l'efficacité opérationnelle.

A ces propriétés essentielles de base, d'autres peuvent être ajoutées. Les variations de ces caractéristiques se retrouvent dans les normes ISO, dans le droit et les standards internationaux ainsi que dans d'autres normes nationales.[Lundgren et al, 2019]

La NIST définit ces trois piliers comme essentiels à tout contrôle efficace qui couvre l'accès, la modification illégale et la continuité des services. Ils sont également perçus comme centraux dans la cybersécurité contemporaine et notamment face aux enjeux de souveraineté numériques et aux proliférations des menaces.

2.3. Pourquoi recourir à la cybersécurité ?

Notre société connait une numérisation massive de toutes ses activités clés ainsi qu'une délocalisation des prestations et une augmentation massive du volume des données. Depuis maintenant deux décennies, les organisations qu'elles soient publiques et privées, dépendent des systèmes d'information pour fonctionner et créer de la valeur. Les SI ne sont donc plus seulement les supports techniques des organisations mais bien le cœur opérationnel de nos activités. Parmi ces fonctions nous trouvons la gestion financière, la communication, le pilotage et bien d'autres encore. [Nehari Talet, 2022] Cette dépendance numérique du monde du travail rend toute interruption ou dysfonctionnement du système potentiellement critique. C'est ainsi ce que souligne [Ponsard et al., 2022] « De nombreux secteurs d'activité sont devenus tributaires de systèmes d'information ou de contrôles industriels pour leur fonctionnement quotidien. Si cela contribue à les rendre plus réactifs, automatisés et compétitifs, la quantité de plus en plus importante de logiciels, combinée à un haut degré de complexité des systèmes et de leurs interconnexions accroît leur exposition aux menaces de cybersécurité. »
Cette ouverture croissante vers la numérisation s'accompagne d'une augmentation considérable des vecteurs d'attaque. En effet les points d'accès aux systèmes des organisations se multiplient rendant les frontières des réseaux de plus en plus floues. Les menaces peuvent émerger de l'intérieur par les employés et les prestataires aussi bien comme de l'extérieur par des acteurs externes malveillants.

2.4. La Maturité cyber

Si la maturité cyber d'une entreprise se définit comme sa capacité à anticiper, prévenir, détecter, répondre et se relever efficacement d'une cyberattaque, elle diffère donc d'une organisation à une autre : En effet elle se mesure et est dictée par la culture de sécurité établie par les organisations. Ainsi, l'implication des dirigeants pour les enjeux de cybersécurité est l'un des moteurs premiers de la maturité cyber.

Or, si l'on s'appuie sur le constat global établi par *Le Baromètre 2024 cybersécurité des entreprises françaises* [Visiativ, 2024], l'on remarque que 70 % des entreprises non pas de référent cybersécurité dédiée. De plus dans l'étude de *PwC* « *Global Digital Trust Insights*

2024/25 » [PwC, 2022] il est énoncé que seules 2% des entreprises estiment avoir une résilience cyber complète dans toute l'organisation. Cela traduit un manque de structuration dans la gestion des risques. C'est en ce sens que « *La cybersécurité est encore souvent perçue comme une contrainte plutôt que comme un levier stratégique*. » [Santos-Neto et al, 2019]. En effet, la plupart des acteurs, notamment les acteurs économiques, n'ont pas pris la mesure des risques et des préjudices associés à l'évolution de la menace numérique. Ces derniers sont souvent traités comme un problème informatique concernant de facto uniquement l'informaticien. Pourtant, [Chavanne, 2017] met en exergue qu'une vraie gouvernance est nécessaire : elle implique une prise en compte des risques au plus haut niveau de management, à l'instar des autres risques identifiés (risques naturels, nucléaires…). Il ajoute que cela doit même s'appliquer dans le cas d'une sous-traitance pour sa sécurité informatique.

2.5. La montée des cybermenaces

La croissance de la numérisation des entreprises s'accompagne proportionnellement d'une augmentation préoccupante des cybermenaces. En effet, aussi bien les collectivités que les organisations publiques et privées deviennent des cibles de choix pour des réseaux malveillants toujours plus organisés

Ces risques cyber ont conduit à une prise de conscience à l'Union Européenne : en effet, le 13 septembre 2017, Jean-Claude Juncker a relevé les faiblesses de l'UE face aux cyberattaques. Les chiffres rapportés par l'UE et analysés par [Knockaert, 2019] sont impressionnants : en 2016, plus de 4000 attaques ont été détectées par jour, et 80 % des entreprises européennes ont connu au minimum un accident [Knockaert, 2019]. De même en 2023, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a recensé plus de 150 incidents majeurs ayant touché directement des organisations publiques et dont une forte part concerne les collectivités territoriales. [ANSSI, 2023] « *L'ANSSI constate un regain du nombre d'attaques destinées à promouvoir un discours politique, à entraver l'accès à des contenus en ligne ou à porter atteinte à l'image d'une organisation* » [ANSSI, 2023] Ces chiffres soulignent un constat sur les cybermenaces « *Leur nombre et leur intensité augmentent d'année en année. L'interconnexion mondiale des systèmes d'information, le volume des échanges internationaux de données et la numérisation progressive de la société y contribuent de manière décisive. Au-delà des services de la société de l'information, tous les secteurs sont touchés* » [Douville, 2020] Chaque évolution s'accompagne ainsi de ses défis. L'évolution numérique ne s'est pas faite sans

contrepartie : elle a ainsi provoqué une guerre contre des ennemis invisibles opérant dans l'ombre du cyberespace.

2.5.1. Des chiffres alarmants

Des chiffres frappants supplémentaires illustrent la montée des cyberattaques et l'intensification de ces menaces. En 2023, l'intervalle entre deux attaques cybercriminelles dans le monde était de 39 secondes. En 2024 l'intervalle consiste désormais en 10 secondes, soit 29 secondes de moins en seulement une année. Ces chiffres mettent en lumière le pouvoir d'attraction, notamment économique, de la cybercriminalité. A des fins de comparaison, il est utile de rappeler que la cybercriminalité a un poids économique plus important que le trafic de drogues. Cela s'explique notamment par le danger moindre pris par les criminels : en effet, leur terrain est un simple bureau. De plus, on estime à 20 000 milliards de dollars le cout de la cybercriminalité en 2026. En 2015 nous étions à 450 milliards. Une progression vertigineuse qui, au regard de la tendance actuelle, ne montre aucun signe de ralentissement. Le cyberespace offre aux auteurs d'attaques un anonymat, une mobilité, une portée géographique et une capacité de nuisance sans précédent. [Walden, 2005]

2.5.2. Les collectivités : une cible privilégiée

Les structures publiques, en particulier les collectivités, sont des cibles privilégiées des cybercriminels. Et pour cause : en raison de leurs infrastructures critiques et leur données sensibles qu'elles traitent, 48% des cyberattaques qui ont été identifiées en 2024 par les autorités compétentes ciblaient des structures publiques (mairie, département hôpitaux, régions). Pendant longtemps, les collectivités ne se sont pas senties concernées par la cybersécurité, mais aujourd'hui elles en sont préoccupées. En 2023, près de 17 % des collectivités qui avaient fait l'objet d'une cyberattaque ont subies une attaque majeure avec un arrêt de service et une perte de données. En 2020, près de 30 % des collectivités territoriales ont été victimes d'une attaque au rançongiciel [Marchand, 2024] Il y a donc une grande multiplication des traitements de données à caractère personnel au sein des collectivités. Cela amplifie le risque de failles et de vulnérabilité qui créé un terrain propice aux cyberattaques. [Marchand, 2024, p.4] Mais pourquoi sont-elles autant ciblées par les attaquants désormais ?

2.5.3. La donnée : l'or noir du cyberespace

La transformation numérique des collectivités, c'est-à-dire le fait d'utiliser des outils numériques, de développer des concepts de relation avec les citoyens, fait augmenter la surface de vulnérabilité des collectivités face aux risques cyber. En effet les collectivités créent et possèdent de la donnée. C'est pourquoi Marchand affirme qu'*« avec l'accélération de la numérisation de l'activité économique et administrative, de plus en plus de données sont produites dans les territoires. Elles font partie intégrante des politiques publiques*. » [Marchand, 2024, p.1]. Cette donnée est considérée comme de l'or noir et est particulièrement recherché par les attaquants.

Les attaquants s'en prennent également aux collectivités à des fins de déstabilisation du fait de leur rôle au sein de la société. De nombreuses raisons sont jugées comme bonnes pour les attaquants : par le biais de l'attaque sur les collectivités ils peuvent promouvoir un discours politique, faire de l'activisme ou encore entraver l'accès à du contenu en ligne. Toutes ces actions affectent l'image d'une organisation, voire la décrédibilise.

2.5.4. Des méthodes diverses et variées pour percer la moindre faille

Les réseaux criminels utilisent de nombreuses méthodes pour arriver à leurs fins : faire du profit. En effet, la montée des attaques répond à la montée de la sécurité, obligeant de fait les trafiquants à trouver de nouvelles méthodes plus élaborées.
C'est pourquoi [Douville, 2020] met en lumière que les attaques sont devenues plus sophistiquées, mieux élaborées, plus destructrices et touchent désormais l'ensemble de la société et des citoyens, entreprises, infrastructures critiques et administration.
Assez paradoxalement, les méthodes les plus simples demeurent les plus utilisées et préférées des cybercriminels.

2.5.4.1.Principales méthodes

Hammeçonnage, rançongiciel, vol de mot de passe, faux sites internet… L'imagination ne manque pas chez les pirates pour attaquer la moindre donnée.

L'hameçonnage (*phishing*), est une méthode qui consiste à faire croire que l'on communique avec un tiers de confiance. Le pirate peut donc se faire passer pour une banque, une mutuelle ou même une administration. La majeure partie du temps, il est effectué par le biais de faux sites internet tels que des site web administratifs. Perfectionnés au fur et à mesure, ils peuvent parfois être la copie conforme de l'original. Le but des attaquants est de récupérer des données de paiement ou des mots de passe qui peuvent nuire aux salariés et aux entreprises. [Ministère de l'économie, 2025] L'hameçonnage est l'une des techniques les plus répandues et le plus utilisées puisqu'elle repose sur l'exploitation de la confiance et la méconnaissance des utilisateurs. Les chiffres soulignent le recours récurrent et le succès effrayant de cette technique. En effet, en 2022, près de 83 % des entreprises interrogées dans une étude ont déclarées avoir été victimes au moins une fois d'une tentative de phishing. Ces attaques particulièrement appréciées des pirates permettent l'intrusion dans les systèmes d'information facilitant ainsi l'installation de *malwares* ou de *ransomware*.[Aleroud et al, 2017]

Les Rançongiciels (*Ransomware*) sont des programmes informatiques malveillants. Le principe consiste à mettre l'ordinateur ou le système d'information hors d'état de fonctionner de manière réversible par le chiffrage de données dans le but d'exiger une rançon en échange de leur déchiffrement. [Ministère de l'Économie, 2025]
Ces dernières années, les attaques ransomware ont explosées à l'échelle mondiale en infectant n'importe quelle victime. Le Ransomware n'est plus l'affaire d'un seul individu, il est devenu un véritable business souterrain structuré. Il mobilise de nombreuses compétences criminelles qui sont dès lors vendues comme n'importe quel service. [O'Kane et al., 2018]

Classique mais pas des moindre, le vol de mot de passe continue de sévir. Il consiste à utiliser des logiciels destinés à tenter un maximum de combinaisons possibles afin de trouver le mot de passe des utilisateurs. Il s'obtient par plusieurs techniques comme en multipliant les essais d'après des informations obtenues par divers moyens. On appelle cela l'attaque par force brute [Staili et al, 2024]. L'objectif final est de récupérer des données personnelles comme professionnelles pour usurper les identités et celles des entreprises. [Ministère de l'Économie, 2025]

La Pandémie de la Covid-19 et le confinement ont conduit à un essor si ce n'est une démocratisation du télétravail qui augmente la vulnérabilité des utilisateurs face aux cyberattaques. En effet de nombreux employés se connectent à des réseaux WI-FI dans le cadre

de leur activité professionnelle. Que ce soit en lieu public, à l'étranger ou en entreprise, une multitude de connexions WI-FI ouvertes provenant de l'extérieur peuvent apparaitre. Cependant il est fort probable que certains réseaux soient piégés. Les bénéfices pour les pirates : la récupération de données sensibles dont le vol pourra nuire aux salariés et aux entreprises. [Ministère de l'Économie, 2025]. Avec ces réseaux WI-FI les attaquants peuvent effectuer plusieurs manœuvres tel que l'espionnage ou l'intrusion tout cela dans le but de voler des informations sensibles. [Staili et al, 2024]

2.5.4.2.Social Engineering

Si autrefois la menace cyber était réellement technique, aujourd'hui la marge de progression ayant radicalement évoluée par des compétences techniques en interne, le principal facteur n'est non plus technique mais humain. C'est ce que démontre Ventre *« En face, il y a des adversaires/ennemis/opportunistes, qui partagent de plus en plus les mêmes dépendances technologiques mais pas nécessairement les mêmes valeurs, intérêts, objectifs, et ont appris à tirer parti de nos fragilités*. » [Ventre, 2015, p.1] C'est pourquoi les attaques par ingénierie sociale représentent les plus grandes menaces pour la cybersécurité : Il n'existe aucun moyen d'empêcher ces attaques puisque les « social engineers » exploitent les victimes afin d'obtenir des informations sensibles qui peuvent par la suite être utilisées à des fins spécifiques ou revendues. Avec l'avènement du Big Data, les données deviennent précieuses notamment pour des fins commerciales. [Salahdine et al, 2019]

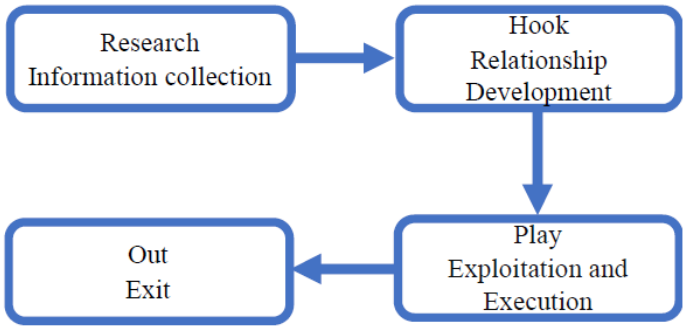

Figure 9 : Social engineering attack stages (Salahdine et al, 2019)

Les « *Social Engineering attacks* » sont effectuées en établissant une relation avec les victimes en jouant sur la psychologie et les émotions comme illustré sur le shéma ci-dessus. Ce sont généralement les attaques les plus dangereuses et les plus efficaces car elles impliquent l'interaction humaine.

Les « *social engineering attacks* » peuvent combiner différents aspects qu'ils soient humains, informatiques, techniques, sociaux et physiques. Parmi les exemples de social engineering attacks, nous pouvons citer l'usurpation d'identité lors d'appels, le « *shoulder surfing* » (regarder par-dessus l'épaule), le « *dumpster diving* » (la fouille des poubelles), le vol de documents importants, le vol par diversion, les faux logiciels, le quid pro quo…[Salahdine et al, 2019] Une quantité de techniques sont ainsi possible par les attaquants pour dérober la moindre information. Il est devenu aujourd'hui quasi impossible d'empêcher totalement la fuite d'informations malgré une architecture technique compétente.

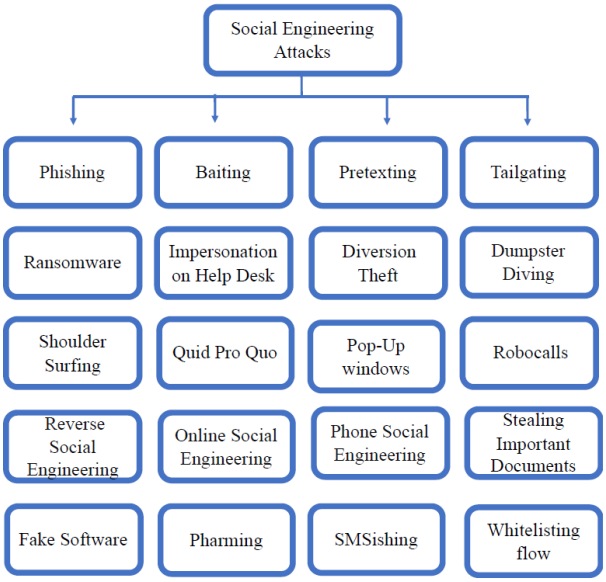

Figure 10 : Social engineering attacks stages (Salahdine et al, 2019)

2.5.4.3.L'humain : maillon faible

Peut-être faut-il rappeler que tout risque, même cyber, se caractérise par une combinaison d'un aléa et d'une vulnérabilité : ici, la vulnérabilité est humaine. En effet, l'une des principales portes d'entrée reste pour les cyberattaques la négligence et l'inattention par les utilisateurs.

Les facteurs humains et organisationnels jouent un rôle important dans l'occurrence de la majorité des accidents, et ce qu'ils s'agissent d'erreurs humaines dans l'exécution d'une action, d'une mauvaise gestion d'interfaces entre services, d'installations insuffisamment résistantes aux erreurs humaines ou bien d'erreurs dans la prise de décision. [Perinet et al, 2010] En effet la plupart des attaques sont réalisés par courrier électronique et 90 % des attaques sont rendues

possibles par les utilisateurs ou par une erreur humaine. Il ne suffit que d'une seule personne pour provoquer des conséquences désastreuses sur l'organisation.

La littérature en cybersécurité souligne largement que les attaques ne résultent plus en majorité d'une vulnérabilité technique mais trouve ses origines dans des comportements humains.
Ces comportements ne sont pas toujours intentionnels : la majorité des incidents relèvent d'une grande méconnaissance, d'une surcharge cognitive ou bien d'un contournement des règles perçues comme trop contraignantes.

Traditionnellement, la cybersécurité a toujours appréhendé le facteur humain sous l'angle de « l'erreur ». Seulement, réduire cette réduction d'une vulnérabilité importante occulte la complexité des contextes organisationnels.
Les travaux de [Nobles, 2018; Garza et al., 2022] proposent de considérer la diversité de ces comportement en deux positions : L'intentionnalité qu'elle soit bénéfique neutre ou malveillante, et le degré d'expertise technique. Cette approche va distinguer les erreurs naïves d'utilisateurs non formés et les conceptions dangereuses réalisées par des experts techniques.

Si les comportements non sécurisés résultent d'une partie de la négligence des acteurs, deux facteurs ressortent quant aux comportements à risques.

Les pressions temporelles et la charge de travail réduisent en partie la capacité cognitive des utilisateurs. Cette distance amène les utilisateurs à éviter ou contourner les mesures de sécurité. Les contraintes telles que les délais ou l'urgence favorisent un climat à risque et rend les individus plus vulnérables aux attaques du type phishing ou ingénierie sociale.

La perception de la cybersécurité est quant à elle reléguée derrière les objectifs de productivité. La cybersécurité peut être estimée comme non prioritaire et décourage à respecter les règles. L'effet contradictoire est donc courant : des mesures trop contraignantes peuvent inciter à des pratiques finalement risquées. [Garza et al., 2022]

Du point de vue des organisations un biais persiste : accorder une confiance excessive dans la technologie. Les entreprises sont dotées de solutions techniques robustes de cybersécurité mais négligent trop souvent la dimension humaine, comportementale et cognitive.

Les recherches mettent en évidence que cette approche « techno déterministe » conduit à ignorer les vulnérabilités humaines. [Nobles, 2018]

2.5.4.4.La Cyber-psychologie

Notre recherche dans la littérature met en évidence que la majorité des incidents ne sont pas dus aux infrastructures techniques mais aux comportements humains inadéquats [Perinet et al., 2014 ; Garza et al, 2022]. Ce constat amène à s'intéresser à une certaine étude du cerveau humain avec les technologies : la cyber psychologie, c'est-à-dire l'étude entre la psychologie humaine et les environnements numériques [Attrill-Smith et al., 2019].

[Norman, 2017] définit la cyber psychologie comme « *Cyberpsychology is about humans and computers and the psychology of how they interact. Computers permeate nearly every human activity in the modern world and affect human behavior from the most basic sensory-motor interactions to the most complex cognitive and social processes* ». C'est donc l'étude scientifique des comportements et pensées associées à l'utilisation des technologies numériques.

Dans le contexte de la cybersécurité, cette pratique permet de comprendre et d'analyser pourquoi les utilisateurs contournent les règles ou a contrario, développent des comportements défensifs.

- Biais cognitifs et vulnérabilités.

  Les recherches en cyber psychologie ont mis en évidence plusieurs biais cognitifs qui impactent la posture des individus face aux risques de sécurité.

  Les premières études menées par Neil Weinstein introduisent le concept de biais d'optimisme en 1980 [Weinstein, 1980]. Il s'agit de la tendance à croire que les utilisateurs sont moins exposés aux cyberattaques que les autres. [Furnell, 2008]. Les utilisateurs ont ainsi tendance à se percevoir moins exposés aux risques négatifs que les autres. Cette tendance se retrouve massivement en cybersécurité. [Rhee et al., 2009] insiste sur l'impact de ce biais qui amène à une sous-estimation des risques et donc une prise en compte des pratiques sécuritaires trop fragiles.

  La fatigue décisionnelle est introduite par [Baumeister et al., 2007]. Elle évoque une rélfexion contradictoire de la part des individus : plus une personne doit prendre des décisions, plus sa capacité à faire de bons choix diminue. Dans le cadre de la cybersécurité, la surcharge cognitive élevée entraine les individus vers des comportements plus vulnérables aux biais et manipulations, un terrain fortement exploité par le phishing ou l'ingénierie sociale.

L'illusion de contrôle, quant à elle, amène à penser que les agents maitrisent leur environnement numérique alors qu'ils ne réalisent pas la complexité des menaces. [Nobles, 2018]. Ceci explique en partie pourquoi la plupart des incidents trouvent leur origine dans les comportements humains.

Ces biais confirment la logique organisationnelle selon laquelle il est nécéssaire pour une politique de sécurité éfficace d'intégrer les motivations, les habitudes et les résistances au changement des utilisateurs. [Sasse et al., 2001].

La cyberpsychologie apporte ainsi une nouvelle méthodologie stratégique. En effet son intégration dans les pratiques de gestion de projet en lien avec la cybersécurité découle une stratégie à trois niveaux :

- La prévention : En tenant compte de tous les risques liés aux biais cognitifs humains, nous pouvons concevoir des dispositifs de sécurité adaptés aux freins identifiés.
- La sensibilisation : Certaines approches issues de la cyberpsychologie (mises en scènes, simulations) se sont révélées bien plus efficaces que des mises en garde classiques.[Parson et al., 2014]
- La gouvernance : comprendre les raisons des comportements à risque permet de batir une culture de sécurité plus efficace et partagée. [Bada et al., 2015]

2.6. Les impacts multiples

Les dommages d'une cyberattaque ne se mesurent pas uniquement au niveau informatique, ils sont considérables. En effet ils peuvent aller de simples désagréments tels que des ordinateurs infectés par un virus, mais aussi à des pertes de plusieurs milliard de dollars pour certaines entreprises, voire à des pertes humaines si certains systèmes critiques sont perturbés. [Walden, 2005]

2.6.1. Impacts sociologiques

Selon l'identité des attaquants et des victimes, les effets psychologiques des cybers menaces peuvent même rivaliser avec ceux du terrorisme traditionnel.

En effet nous pouvons analyser une palette très large des états psychologiques que peuvent subir les salariés après une cyberattaques. Cela peut se traduire par l'anxiété, la colère, la dépression ou encore la honte et la culpabilité ainsi qu'une perte de confiance en soi. [Ferguson-Walter et al., 2021].

Prenons également l'exemple du vol d'identité sur une victime. Cela peut engendrer de la détresse de la part de cette personne qui se sentira violée, trahie, vulnérable ou encore impuissante. Les victimes peuvent entrer dans des phases de deuil ou encore souffrir de colère ou de rage. Dans certains cas, celles-ci peuvent même se blâmer et développer un sentiment de honte. [Woods et al., 2017]

2.6.2. Impacts sur les collectivités

Les impacts d'une cyberattaque sont multiples et ce, bien loin de la simple sphère informatique. Lorsqu'une collectivité est victime d'une attaque, cela concerne l'ensemble de ses services et missions. Cela peut engendrer un dysfonctionnement, voir l'arrêt des services publics locaux, de l'urbanisme, des retards dans la gestion des éléments qui viennent donc altérer le lien de confiance avec les administrés. Mais, cela affecte aussi la gestion des infrastructures publiques tels que l'énergie, les éclairages, la sécurité de l'espace public avec les vidéos protections et l'accès sécurisé à certains bâtiments. Le bon fonctionnement interne de certains services tel que le vote peut être touchés, mais aussi les Ressources humaines qui gèrent les règlements de paye, les éditions de factures, les paiements… Bien évidemment, cela a un impact majeur en termes de pertes de données personnelles et ce de manière parfois irréversible. De fait, les cyberattaques sur les collectivités entraînent des conséquences directes sur les citoyens puisque leurs données sont utilisées à des fins malveillantes.

L'attaque peut également se répercuter sur les agents notamment au niveau du stress avec des conséquences visibles qui sont le départ des agents. Bien évidemment l'impact en termes d'image est considérable. La confiance est une vertu qu'une collectivité ne saurait perdre.

2.7. Les Exigences en cybersécurité : Une régulation croissante pour structurer la réponse organisationnelle

2.7.1. Une genèse règlementaire avant tout

La cybersécurité n'est pas simplement née d'une démarche spontanée mais d'un cadre réglementaire imposé. En effet, 90% des organes de sécurité au sein des entreprises sont apparus à la suite d'obligations légales. Le développement de tous ces métiers axés sur la sécurité s'est opéré autour de la nécessité de protéger les systèmes imposés par la loi.
Il existe aujourd'hui de nombreux guides, méthodes, normes, recommandations ou règlementations qui abordent les enjeux de cybersécurité à un niveau industriel. [Masse et al., 2017] A travers l'analyse de nombreuses stratégies, plans ou encore programmes sur le sujet de la cybersécurité et cyberdéfense de ces dernières années, une certitude commune se dégage : il est désormais essentiel et reconnu qu'il est indispensable d'organiser et de garantir la sécurité et la défense de l'espace numérique. Cela implique dans un premier temps la protection de systèmes techniques mais également des sociétés qui en dépendent profondément. Un constat : la sécurité des systèmes d'information conditionne celle de l'état nation. [Ventre, 2015]

2.7.2. CNIL

Créée par la loi Informatique et Libertés du 6 janvier 1978, la Commission nationale de l'informatique et des libertés (CNIL) est aujourd'hui au cœur des problématiques modernes.

Le rôle de la CNIL est de réguler les données personnelles. Il s'agit de la première législation en France en matière de protection des données informatiques. Secouée par les enjeux du monde en perpétuel évolution et sujet aux transformations numériques, aux crises sanitaires, aux risques cyber et la multiplication des flux de données, elle doit s'adapter et appréhender ces mutations avec agilité en renforçant ses capacités de régulation et d'accompagnement face à des usages numériques toujours plus complexes et interconnectés. [Maury, 2022]

En tant que garante du respect de la vie privée et des libertés individuelles et publiques françaises, elle veille à ce que le développement technologique s'effectue dans le respect des personnes concernées. [Bertaud du Chazaud et al, 2020]

Au quotidien la CNIL informe, conseille, contrôle et sanctionne. Elle est l'acteur de référence en matière de protection des données personnelles. Celle-ci se place en tant qu'autorité de sanction dans les cas les plus graves. Sa démarche est d'avant tout conseiller les bonnes pratiques et les bonnes actions à mener pour être au plus proche de la conformité. [Leto Legal, 2022]

2.7.3. ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), crée en 2009, est une autorité nationale en termes de cybersécurité et de cyberdéfense. En France, elle fait partie des services du Premier Ministre au sein du Secrétariat général de la sécurité et de la défense nationale. Elle est donc placée à proximité du sommet de l'exécutif et a comme mission unique et exclusive la cybersécurité. Les rôles et missions de l'ANSSI sont exclusivement défensifs. Elle veille à proposer les solutions les plus adéquates pour les particuliers, les entreprises et les administrations. [Strubel, 2023] L'une des missions principales est de mener des actions de sensibilisation en s'adressant à l'ensemble des acteurs clés de la société du numérique et créer une culture de la cybersécurité. [Chavanne, 2017] Plus concrètement, l'ANSSI s'efforce de mieux comprendre les menaces qui cherchent à porter atteinte aux intérêts français. Elle s'attache à détecter les attaques et en particulier celles ciblant l'Etat afin de pouvoir intervenir rapidement, y mettre un terme et restaurer le système d'information dans un état suffisamment stable pour continuer l'activité.

2.7.4. LCEN

La LCEN (Loi pour la Confiance dans l'Economie Numérique) est une loi française promulguée le 21 juin 2004. Elle vise à encadrer le développement d'Internet et du commerce électronique en garantissant les droits des internautes et la responsabilité des acteurs du numérique. [CGV-Expert, s.d.] Elle constitue une transposition de deux directives européennes qui font référence à la protection des données personnelles dans les communications électroniques ainsi qu'au commerce électronique et digitale. Cette loi s'adresse au monde d'internet, donc aussi bien aux hébergeurs qu'aux vendeurs, consommateurs, prestataires techniques, aux internautes, au cybercommerçants… Chaque personne évoluant dans le milieu de la communication et du commerce électronique sont concernées.

La loi LCEN repose sur deux principes fondamentaux : la liberté d'expression et la protection des droits individuels. Elle « *fixe le cadre légal d'exercice des activités de commerce électronique, des services en ligne et des prestataires Internet* » [service industrie, s.d.]

2.8. Règlements

L'encadrement juridique de la cybersécurité de ne se limite pas simplement à des institutions nationales telles que la CNIL, l'ANSSI ou la LCEN. L'encadrement s'inscrit également dans une dynamique de réglementation au niveau européen et international. L'objectif de cette réglementation est d'harmoniser les pratiques, de renforcer la résilience des espaces numériques et de garantir la protection des droits fondamentaux alors que nos pratiques quotidiennes et professionnelles sont de plus en plus numérisées. Ces différents règlements viennent consolider les obligations légales existantes en y apportant les dimensions opérationnelles, plus contraignantes et le plus souvent transversales.

2.8.1. RGPD

Dans un ouvrage consacré à la Cybersécurité et le traitement des données personnelles par les collectivités territoriales, Marchand met en évidence que « *Lorsque les données revêtent un caractère personnel, des règles de traitement précises et rigoureuses doivent être mises en place par les collectivités territoriales dans le respect du RGPD* » [Marchand,2024, p.1]. Aujourd'hui il devient difficile d'échapper à l'utilisation d'objets électroniques connectés tels de que des ordinateurs et des outils reliés à internet. Cependant ces évolutions d'outils nécessitent une grande consommation et échanges de données personnelles. En entreprise et dans la vie personnelle l'exploitation des données personnelles est devenue indispensable au fonctionnement même de nouveaux services. Leur importance économique et croissante est non-négligeable. Lorsque l'on évoque les réseaux sociaux, la relation client, les comptes en ligne, la connaissance de l'utilisateur et du client est un élément essentiel.
Désormais, avec la multiplication de ces échanges de données, le traitement des données à caractère personnelle représente un enjeu crucial pour les entreprises et organisations. Les données sont omniprésentes et doivent être traitées et protégées dans les formes prescrites par la loi. [Mattatia, 2019] Le règlement général sur la protection des données (RGPD) responsabilise donc les organismes publics et privés qui traitent leurs données. « Ce règlement

concerne l'ensemble des structures susceptibles de recueillir les données personnelles pour les conserver et par la suite les exploiter afin de proposer ou de développer des offres de produits et/ou de services. « *Il s'agit de la mise en place d'un cadre légal, vis-à-vis de tout organisme, qu'il soit situé ou non dans l'Union européenne, du moment qu'il exploite les données personnelles de citoyens européens.* » [Boulesnane et al., 2020, p.104] La mise en conformité doit se faire en plusieurs étapes et doit être suivie au sein de n'importe quelle organisation. La CNIL apporte une aide et un soutien précieux pour l'accompagnement de conformité au RGPD. Il est nécessaire de mettre en place un processus codifié pour respecter les exigences liées aux données personnelles.

Tableau 1
Synthèse du référentiel d'aide à la conformité de la Cnil

Étape 1 **«Désigner un pilote»**	Désigner un DPO (conduite de la conformité au règlement) Diversité des rôles : contrôle interne, information, communication, veille
Étape 2 **«Cartographier»**	Tenue d'un registre de traitement : Coordonnées des acteurs chargés du traitement des données Liste des activités de traitement (qualification, finalité, personnes concernées, catégories de données, données sensibles) Lieu d'hébergement des données Durée de conservation des données Mesures de sécurisation appliquées
Étape 3 **«Prioriser les actions»**	Partir du registre de traitement : Définir, pour chaque donnée, les actions à mener Prioriser des actions (en fonction du niveau de risque) Importance du traitement de données sensibles
Étape 4 **«Gérer les risques»**	Identifier les risques (sur la base de 9 critères) Mettre en place d'une Analyse d'impact relative à la protection des données (AIPD) : obligatoire si deux traitements sont détectés
Étape 5 **«Organiser»**	Prendre en compte les risques Intégrer la sécurisation dès la conception des systèmes Protéger les droits liés à la liberté individuelle
Étape 6 **«Documenter»**	Justifier la conformité au règlement Constituer une documentation (registre de traitement et AIPD) Rôles et responsabilités des acteurs

Figure 11 : Tableau de référentiel d'aide à la conformité de la Cnil (Boulesnane et al., 2020)

2.8.2. NIS 2

La directive NIS 2 (Network and Information Security), adoptée en décembre 2022, marque un tournant dans la construction d'un espace numérique européen sécurisé. Cette nouvelle directive succède à la NIS de 2016 et vient répondre aux manquements de celle-ci. La nécessité d'évolution de la NIS vient du constat que les cybermenaces nécessitent une réponse plus structurée et homogène à l'échelle de l'Union Européenne. Ce changement s'inscrit dans une volonté politique de renforcer la résilience des services numériques critiques dans tous les Etats-membres. [Salvaggio et al, 2023]

L'objectif de l'évolution de la NIS est d'adapter le cadre réglementaire face à l'ampleur des menaces modernes. C'est pour cela que NIS 2 élargit considérablement le périmètre des entités concernées. Ce sont désormais toutes les entités exerçant une activité jugée critique selon des critères propres. Deux entités sont identifiées : les entités « essentielles » (hôpitaux, fournisseurs d'eau et d'énergie…) et les entités « importantes » (industries, agroalimentaire…). [Directive NIS 2, 2022].

La mise en place de NIS 2 s'accompagne bien évidemment d'un renforcement en matière de cybersécurité. Il est désormais essentiel de mettre en place des politiques de sécurité adaptées pour assurer la gestion des risques, sécuriser les infrastructures et garantir la continuité des activités. En cas d'incidents, les infrastructures sont tenues de le notifier à l'autorité compétente dans un délai de 24 heures. [Directive NIS 2, art.23]. La cadre se veut désormais plus contraignant et plus opérationnel, avec une volonté forte de réactivité face aux incidents.

Par cette nouvelle évolution, les autorités nationales joueront un rôle renforcé. C'est le cas de l'ANSSI. Elles seront chargées de superviser les entités et de contrôler la conformité à travers des audits. En ce sens, l'ANSSI détiendra un pouvoir et de réglementation et de sanction pour accroitre son efficacité. [Directive NIS 2, art. 34]. L'autorité nationale devient ainsi un acteur central garant de la bonne application du dispositif sur le territoire français.

Enfin, une volonté européenne d'encadrer le numérique de manière souveraine émerge de plus en plus dans l'environnement numérique des pays. La NIS 2 n'est pas une, elle s'inscrit dans un écosystème réglementaire plus large qui inclut le RGPD, le Cybersecurity Act et le Cyber Resilience Act. [ANSSI, 2023].

2.8.3. Donner du sens aux exigences réglementaires

Si cette multiplication des réglementations peut donner une impression de complexité croissante pour les acteurs publics, chacune de ces réglementations répond à une certaine logique précise avec des objectifs complémentaires.

Par exemple, le RGPD vise à instaurer une culture de confiance et de protection des données personnelles en renforçant les droits des citoyens et en responsabilisant les organisations. [Règlement général de la protection des données ; CNIL, 2016] La directive NIS 2, s'inscrit quant à elle dans une logique de résilience des infrastructures numériques et impose des mises en place aux entités publiques permettant la gestion proactive des risques et incidents.

Ces deux règlementations s'influent mutuellement, en effet le RGPD protège la donnée en tant qu'actif sensible tandis que la NIS 2 protège l'infrastructure numérique qui traite et héberge ces données. Ensemble elles poussent les organisations à établir une culture de prévention et de sécurité.

2.8.4. De possibles tensions entre le niveau national, européen et mondial

Le paysage règlementaire français en matière de sécurité et de protection des données est perçu comme dense et complexe, notamment pour les collectivités.

Pourtant toutes ces réglementations poursuivent l'objectif de contribuer, chacun à sa manière, à la construction d'un environnement numérique plus sûr et plus fiable. Leur articulation est censée fournir un cadre cohérent qui vise à accompagner et non à contraindre dans la transformation numérique des organisations. [Kianpour et al, 2024]

Cependant ces architectures n'exclues pas toutes tensions. En effet les réglementations nationales doivent s'articuler en même temps que les directives européennes qui sont-elles même influencées par des standards internationaux. Ce chevauchement peut engendrer des difficultés d'interprétation et de mise en œuvre. En effet une collectivité doit simultanément répondre à des obligations française, européennes et à des référentiels internationaux parfois utilisés par les prestataires. [Dupont, 2017] Cette superposition peut engendrer un effet de complexité ou la cohérence voulue est perçue comme une surcharge normative.

Loin de former une simple juxtaposition de normes, ces réglementations sont censées protéger les usagers et garantir la continuité des missions de service public. L'enjeu est de dépasser la perception de la contrainte et de comprendre comment les articuler en différents niveaux

normatifs pour renforcer la maturité numérique. La cybersécurité est une responsabilité multicouche traversant les niveaux organisationnels et les standards globaux. [Panteli et al., 2025]

2.9. Cadre législatif utopique

Comme nous avons pu le souligner nous assistons à une inflation normative continue depuis le début du XXIe siècle. Les exigences en matière de cybersécurité se sont considérablement accrues et notamment au cours des années 2000. Cela se traduit par une multiplication des normes, règlements et référentiels techniques. Tout cela est ainsi le résultat d'une volonté politique et stratégique afin de sécuriser les systèmes numériques désormais présents dans tous les domaines. Ces systèmes sont désormais considérés comme des actifs critiques des organisations pour la continuité des services publics et privés. La prolifération de ces textes créé un environnement réglementaire complexe et instable difficile à suivre pour les acteurs opérationnels. En effet derrière cette importante quantité de règles, l'alignement entre l'ambition stratégique portée par les autorités et la réalité concrète de mise en œuvre par l'équipe projets sur le terrain est de plus en plus mise sous tension. Il est impossible de tout appliquer simultanément qui plus est avec les ressources humaines, financières et techniques disponibles dans les organisations. Les organisations se retrouvent à faire des choix entre conformité juridique, faisabilité technique, contraintes budgétaire et disponibilité des compétences [Hoffmann et al., 2020]. [Hoffmann et al., 2020 & Cheimondis et al., 2023] soulignent l'approche probabiliste de la cybersécurité, fondée sur un raisonnement en termes de risques acceptables. Cela confirme qu'il faut concevoir des protections proportionnelles aux enjeux. Les chefs de projet sont donc au cœur de ces tensions et doivent assurer la livraison des projets tout en intégrant les enjeux de cybersécurité sans que les logiques soient toujours alignées. Dans les faits, la sécurité devient un paramètre à gérer parmi d'autres au même titre que la performance fonctionnelle ou les délais. Elle reste intégrée mais mise en tension par les impératifs de dates, les attentes fortes ou les contraintes politiques. Ce constat est particulièrement présent dans les structures publiques soumise à des objectifs souvent contradictoires. [Gollmann, 2011] appuie ce constat en rappelant que la sécurité parfaite n'existe pas et n'est qu'une illusion conceptuelle.

2.9.1. La structure : point faible de la sécurité

L'analyse de modèle pyramidal réalisée dans le contexte met en lumière une réalité paradoxale. Comme illustré et évoqué dans cet état de littérature, la plupart des organisations aujourd'hui sont encadrées par les éléments de structuration supérieurs tels que les nombreux Framework, les politiques de sécurités ou encore les standards. Ces éléments internationaux et nationaux constituent des cadres de références solides et indiscutables. Cependant le dernier étage du modèle reste fragmenté. En effet les procédures et contrôles techniques concrets sont paradoxalement bien moins matures que les modèles d'exigences. Cet aspect de la cybersécurité est fragile et documenté de manière trop faible. Or, ce niveau est essentiel pour une efficacité des mesures de cybersécurité. C'est en effet celui qui assure l'effectivité de la sécurité au quotidien. Sans une procédure claire des affectations et missions, les politiques de sécurité restent théoriques. Ce manque de mesures opérationnelles empêche la traduction de la cybersécurité en pratiques partagées. La structuration est donc présente dans les faits, sollicitées dans les politiques mais bien souvent non déployées sur le terrain ou elle est pourtant décisive. [Chavanne, 2017] appuie ce constat du manque de structuration causé par des responsabilités floues dans les équipes responsables des enjeux de cybersécurité. Cette gouvernance fragmentée est un frein à l'adoption d'une gestion cohérente du risque cyber.

2.10. Conclusion de la section

À travers cette deuxième partie dédiée à la cybersécurité, nous avons mis en lumière son évolution, passée d'un enjeu purement technique à une problématique systémique touchant l'ensemble des systèmes d'une organisation. L'émergence des menaces ainsi que la multiplication des régulations et normes illustre une dynamique où la cybersécurité n'est plus uniquement réservée aux experts. En effet, c'est désormais une responsabilité partagée à tous les niveaux organisationnels. La cybersécurité s'inscrit alors à l'intersection de plusieurs dimensions : technologique, juridique, économique et socio-politique.

La cybersécurité doit désormais être intégrée comme un système global, exigeant une gouvernance claire, une acculturation progressive des acteurs et une bonne articulation entre les exigences réglementaires et les pratiques opérationnelles. Ces parties précédentes posent ainsi les bases pour interroger, dans la suite du mémoire, la manière dont les exigences de

cybersécurité sont construites et mises en œuvre dans des contextes tels que les collectivités territoriales.

3. La construction fragile des exigences de cybersécurité

Les exigences de cybersécurité sont donc un ensemble transversal de toutes les contraintes et précautions destinées à protéger les systèmes d'information et les données critique d'une organisation.

Nous pouvons classer les exigences de cybersécurité comme une exigence non-fonctionnelle, première raison de son manque d'application, par ses fonctions qui ne concernent pas directement les fonctionnalités du système et ne répondent pas aux besoins des utilisateurs finaux.

Toutefois, dans de nombreux projets numériques les exigences en termes de sécurité sont mal identifiées ainsi que mal intégrées dans les processus opérationnels.

Nous pouvons expliquer ce constat par plusieurs hypothèses récurrentes. Dans un premier temps la cybersécurité est essentielle par son caractère transversal. Celle-ci couvre toutes les fonctions d'une organisation et pour son efficacité, doit être étendue à chaque système d'une entreprise. La cybersécurité se traduit ainsi par son interdisciplinarité et l'étendue de son champ d'action. [Delorme, 2023]

Les entraves à une intégration proactive de la cybersécurité se traduisent également par une complexité trop technique. [Kremer et al., 2019] expliquent « *La première étape de la cybersécurité consiste à identifier les menaces et à définir une politique de sécurité. Ces menaces peuvent cibler le matériel, le réseau, le système d'exploitation, les applications ou les utilisateurs eux-mêmes Des mécanismes de détection et de protection doivent être conçus pour se défendre contre ces menaces.* » Cependant ces conceptions s'appuient sur des protocoles de cryptographie, qui est un aspect technique de développement de la cybersécurité pouvant paraitre bien trop complexe pour les équipes métiers. En ajoutant les termes et notions propres à la cybersécurité, sa compréhension se retrouve fortement impactée par les personnes non familières ou sensibilisées aux différents termes. Ces termes sont répartis en plusieurs référentiels difficilement traductibles.

La cybersécurité comme beaucoup d'aspect techniques regroupe un langage technique parfois uniquement compris par les experts. En effet les aspects de sécurité mobilisent un lexique complexe. Nous pouvons citer les nombreux mots de vocabulaire technique ; SOC, SIEM, Threat intelligence, EDR… Vient se rajouter les normes et réglementations également complexes à traduire comme ISO 20000-1. Ces termes, à moins d'un apprentissage régulier, restent opaques pour les non-experts. Comme l'expliquent [Ramirez et al, 2016] « *Il existe un fossé en matière de communication dans le domaine de la cybersécurité, qui sépare la recherche technologique traditionnelle et les activités non techniques des secteurs public et privé*. » Cela découle du fait que la Cybersécurité repose sur un langage hautement spécialisé qui est à la fois issue de l'ingénierie réseau, de la gestion des risques mais également de la doctrine militaire renforcée par le fait que les référentiels sont eux-mêmes formulés dans un langage juridique technique.

Ce manque de compréhension n'impacte pas simplement la traduction des exigences mais découle sur la gouvernance même de la cybersécurité qui empêche sa déclinaison en processus clairs. [AlGhamdi et al., 2020] En effet celle-ci est victime d'un cruel manque de gouvernance claire pour porter les exigences. Selon [Villamizar et al., 2018] les exigences de sécurité sont encore trop peu prises en compte dès la phase d'analyse de de besoins des projets. L'étude montre qu'une grande majorité des équipes n'intègrent pas la sécurité de manière formelle dans le processus d'ingénierie des exigences considérant ces notions comme externes au cœur fonctionnel du projet. La cybersécurité est reliée au rôle de couche additionnelle, à intégrer a posteriori, plutôt qu'à sa réelle nécessité d'intégration structurée dès la phase de conception.

[Mohamad et al., 2024] présentent dans leur étude un cas concret mené dans le secteur automobile. Le constat est clair : les preuves de conformité aux exigences de sécurité sont en grande majorité absentes ou incomplètes. Ceci découle du manque de procédures formelles et de l'absence de documentation rigoureuse. Les auteurs interpellent sur une constatation frappante : « *même dans les environnements hautement régulés, les pratiques liées à la cybersécurité restent largement artisanales* ».
Les exigences non-fonctionnelles sont donc des indicateurs à prendre en compte de manière appliquée et rigoureuse pour assurer la structure des exigences non-négligeable telle que la sécurité.

Enfin les référentiels standards tels que ISO/IEC 27001, ont été créés mais non dans une optique de réalité alignée avec celle du terrain opérationnel. La transformation numérique rend les exigences de sécurité de plus en plus critiques mais les structures procédures sont bien trop insuffisantes dans les organisations et mal intégrées dans les projets. [Saeed et al., 2023]
Malgré l'abondance des documents normatifs, de chartes et de guides, les exigences de cybersécurité restent continuellement non contextualisées, non priorisées mais également mal appropriées par les équipes du projet. Cette lacune en termes de clarté procédurale et de gouvernance définie, constitue l'un des freins majeurs à l'intégration efficace dans le pilotage des projets.
[Saeed et al., 2023] insistent là-dessus :« *At the planned level of our framework, organizations need a well-planned organizational cybersecurity strategy documenting the processes for cybersecurity preparation, deployment, and surveillance.* »

3.1. Stratégies de cybersécurité et gouvernance dans les organisations modernes

Dans cette étude approfondie, [Abrahams et al., 2024] fournissent une analyse des différentes évolutions des stratégies de cybersécurité établies dans les organisations de toutes tailles et de tout secteurs. Nous allons ainsi comprendre comment les entreprises conçoivent et implémentent leurs approches de cybersécurité. Cette analyse permet ainsi de mettre en lumière les écarts entre la stratégie affichée et les pratiques effectives au cœur du terrain.
Cette étude qualitative permet une vision concrète des dynamiques organisationnelles en jeu.
L'étude se base sur 6 organisations de secteurs critiques (Financier, santé, énergie, administration publique et télécommunication). La similarité de ces organisations résulte dans des obligations réglementaires fortes.

L'analyse permet d'identifier les mécanismes mis en place pour piloter la cybersécurité au sein des secteurs critiques, les ruptures entre les stratégies, les procédures internes et la réalité du terrain. Et pour finir l'impact du facteur humain dans cette équation.
Le constat est conforme aux problématiques de cybersécurité : bien que la cybersécurité soit tout de même reconnue comme une priorité stratégique, sa mise en œuvre est fragmentée et très peu structurée dans la grande majorité des cas.
Nous pouvons identifier trois tendances fortes :

- Les stratégies sont énoncées par les dirigeants mais peu traduites en actions concrètes. Les politiques de sécurité sont belles et bien existantes mais trop souvent non suivies de plans d'actions et de procédures consolidées. « *Most organizations had well-written cybersecurity strategies, but lacked clear implementation roadmaps or ownership structures* » (Abrahams et al., 2024, p.5).

- La gouvernance de cybersécurité est cloisonnée et entraine une distance cognitive. En effet on cantonne encore trop la sécurité à une direction technique séparée des métiers et du management opérationnel. Cet éloignement cognitif entre les experts et les chefs de projet entraine un effet de silos et accentue l'aspect de contraintes des exigences de cybersécurité.

- Le pilotage des exigences de cybersécurité manque de suivi et d'apprentissage organisationnel. Malgré la conscience générale sur l'augmentation des risques cyber, trop peu d'organisations mettent en place des mécanismes d'évaluation réguliers de leur posture de cybersécurité ni des dispositifs de sensibilisation et d'apprentissage. La reconnaissance des risques par les acteurs reste pourtant l'un des leviers majeurs pour réduire les menaces de cybersécurité.

Cette étude relève donc le paradoxe présent dans de nombreuses entreprises : chacune affiche une volonté forte de renforcer les dispositifs de cybersécurité mais très peu sont capables de traduire cette volonté en exigences concrètes et pilotées.

3.2. Vers une gouvernance mature des exigences cyber

L'étude produite par [Ardi et al., 2023] s'inscrit dans une démarche exploratoire d'intégration, de manière pragmatique d'une évaluation des risques en cybersécurité. La particularité est que cette démarche s'inscrit dès les phases en amont de l'ingénierie des exigences.
Appliquée en grande entreprise suédoise du secteur des télécommunications, cette recherche met en lumière les résistances organisationnelles, les ajustements nécessaires ainsi que les bénéfices d'une démarche d'intégration proactive.

L'organisation ciblée dans cette étude disposait préalablement d'une maturité relativement élevée en termes de gouvernance IT. Cependant malgré cela, elle se heurte un à un problème structurel récurrent dans tout type d'organisation : les exigences de cybersécurité ne sont que très peu prises en compte dans le projet numérique lors de la définition des besoins. Le constat est équivalent aux observations, elles sont intégrées en fin de cycle, uniquement sous la forme de contrôle techniques ou d'audits ponctuels. Ce mode de fonctionnement est implanté dans de trop nombreuses entreprises et cause des retards imprévus, des conflits de priorité, voire des vulnérabilités.

L'objectif de l'expérimentation est simple : établir une approche légère d'analyse de risque directement intégrée au processus d'ingénierie des exigences. Pour cela il suffit de fournir aux analyses métier des outils simples et opérationnels qui permettent d'identifier les potentiels scénarios de menaces, les probabilités ainsi que de déterminer les exigences cyber adaptées à ces risques.

La méthode d'application est restée très simple et à portée de tout employé. Une méthode qualitative fondée sur une observation directe des ateliers d'ingénierie des exigences, des entretien semi-directifs avec les parties prenantes du projet ainsi qu'une évaluation comparative avant/après de l'introduction de l'outils de gestion des risques.

Cette étude relève plusieurs constats clés. Premièrement une amélioration immédiate de la qualité des exigences fonctionnelles est relevée. Les exigences cyber particulièrement, sont devenues plus concrètes et contextualisées. Cette formalisation a également entrainé une appropriation accrue par les équipes techniques. L'écart cognitif entre les métiers et les notions de sécurité a ainsi été réduit permettant une meilleure communication interdisciplinaire.

L'introduction de cette démarche stimule une remise en question du processus global d'intégration des exigences non-fonctionnelles au cœur des projets, ouvrant la voie à une réflexion plus large sur le sujet de procédures internes.

Malgré ces bénéfices observés, les résistances organisationnelles peuvent persister. Des équipes peuvent toujours percevoir cette démarche comme une surcharge méthodologique mais également comme une charge qui n'incombe qu'aux responsables directs tels que les RSSI. Il est donc de rigueur d'établir un processus n'impliquant pas de surcharge et améliorant le pilotage des projets en termes de sécurité, le manque de structuration procédurale découlant majoritairement de défaut d'outillage et de culture projet partagée.

3.3. Gestion des exigences et gouvernance des actifs

L'étude menée par [Alexander, 2024] porte sur la mise en place d'un système de gestion des actifs et des exigences de cybersécurité dans un environnement complexe et à fort enjeux tel qu'un centre médical américain.

Cette démarche vise à illustrer concrètement la manière dont les établissements de santé, soumis à des obligations réglementaires très fortes et confrontées à des enjeux critiques de données, peuvent fortifier leur posture de cybersécurité à travers une structuration des processus internes.

L'hôpital concerné comprend près de 1000 employés confrontés à une numérisation accélérée. Bousculé par ces multiples innovations, le personnel fait face à un manque criant de visibilité sur ses actifs numériques et physiques, rendant ainsi la gestion des risques, la conformité réglementaire et la détection des incidents plus ardue.

Ce projet a pour objectif d'établir un cadre structuré pour la gestion des actifs informationnels afin d'y intégrer les exigences de cybersécurité de leur établissement jusqu'à leur déploiement et vérification.

Les résultats de cette recherche ont été analysés à partir d'une observation détaillée des pratiques internes, d'entretiens avec les responsables sécurité, la DSI et les équipes cliniques.

Cette étude offre la description de mise en place d'un inventaire centralisé des actifs. Cet inventaire comporte : une classification des données (confidentielle/sensibles/publiques), une catégorisation des systèmes utilisés dans les services (appareils médicaux, services, logiciels), ainsi que les exigences de sécurité associées à chaque catégorie (accès, chiffrements).

Par la suite, une procédure formalisée a été introduite pour la mise en service de nouveaux équipements et systèmes. Celle-ci inclut :

- Une évaluation des risques cyber associés
- La désignation d'un propriétaire d'actif
- La documentation des exigences de sécurité applicables
- Le contrôle périodique de conformité

L'étude met ainsi en évidence plusieurs résultats significatifs.

Une nette amélioration de la visibilité et du pilotage, une réduction de la surface d'attaque par la réduction des points d'entrée potentiels, et enfin une appropriation progressive par les métiers grâce à une démarche pédagogique et progressive instaurant une culture partagée de la sécurité.

« *Asset security is a fundamental process for an enterprise. By managing the assets, through identification and categorization, the enterprise can maintain asset security very well and identify any threats to the assets*. »

Des limites restent néanmoins identifiables causés par trois aspects récurrents : la surcharge documentaire perçue, le manque de temps du personnel soignant et la complexité des normes à traduire en procédure terrain.

3.4. Le métier de cybersécurité : une intelligence contextuelle

Les métiers de la cybersécurité ne reposent pas essentiellement de la mise en œuvre de solutions techniques ou du respect formel des normes et référentiels. Il est désormais nécessiteux d'une intelligence contextuelle, c'est-à-dire la capacité à évaluer en permanence à quel moment une organisation est réellement en risque et quelles sont les mesures nécessaires à prendre. L'intelligence de ce métier repose sur le choix de solutions adaptées au contexte de l'organisation et aux besoins réels. « *Viser trop bas expose l'organisation à des conséquences qu'elle ne pourra peut-être pas assumer. Viser trop haut engendre des coûts injustifiables.* » [Paul et al., 2021] Autrement dit ce n'est pas nécessairement un empilement de procédures, mais un travail d'arbitrage afin d'identifier les menaces pertinentes, hiérarchiser les vulnérabilités et ajuster les réponses en fonction du contexte de son organisation. [Paul et al., 2021] renforce cette idée en assurant que « l*e besoin de sécurité est intrinsèquement lié au domaine d'activité*. » Il n'existe pas de modèle universel, chaque structure, possède une exposition spécifique aux menaces.

Le métier de la cybersécurité consiste donc à prendre l'essentiel de ce qui est nécessaire. « *La première étape pour l'identification du besoin consiste à sélectionner, avec les experts métier, les critères de sécurité pertinents.* » [Paul et al., 2021] La sélection des critères à travers une abondance normative est un travail de stratégie complexe qui demande des traductions pragmatiques et adaptées.

Cette logique rejoint la notion d « obligation de moyens ».

Définit par l'article 1231-1 du code civil, l'obligation de moyen est une obligation du débiteur de déployer ses meilleurs efforts pour atteindre l'objectif visé et en respectant les règles de l'art. Dans cette même optique, en termes de sécurité, une organisation doit démontrer qu'elle a mis en place des protection suffisante et appropriées sans pour autant pouvoir garantir une sécurité infaillible, illusoire dans les faits. [Gollmann, 2011]

Par ailleurs, si les solutions technologiques actuelles sont taillées pour répondre aux vulnérabilités, la principale source de risque demeure humaine. Comme rappelé par [Perinet et al, 2014], la grande majorité des incidents découlent d'erreurs humaines et d'inattentions. La cybersécurité repose alors aujourd'hui sur un besoin de formation et de sensibilisation des utilisateurs. Ceux-ci représentent le maillon le plus fragile mais également le plus décisif de la chaine de sécurité. En ce sens la responsabilité des métiers cyber requiert de la formation et l'établissement d'une culture organisationnelle de sécurité.
Par cette analyse nous démontrons une portée stratégique de la cybersécurité. Il s'agit plus de faire appliquer les règles mais d'opérer un travail d'anticipation, d'accompagnement et lisibilité.

3.5. Enjeux, opportunités et pistes d'évolutions

L'analyse de la littérature met en évidence le décalage persistant entre le foisonnement normatif en matière de cybersécurité et sa traduction concrète dans la gestion opérationnelle des projets numériques.
Si chaque organisation est désormais exposée aux cybermenaces, les exigences de cybersécurité demeurent illisibles, fragmentées et mal intégrées dans les pratiques du terrain.

A travers cet revue de littérature, nous avons pu identifier plusieurs constats majeurs.

- Le monde du numérique fait face à une multiplication des exigences réglementaires et a, par la suite, créé un environnement de conformité dense mais peu adapté aux réalités du terrain.

- Les acteurs ont évolué, et notamment le rôle du chef de projet, porteur des exigences projets, s'est profondément transformé. Il est devenu un acteur stratégique au croisement des dimensions techniques, organisationnelles et humaines. Garant de certaines exigences, il n'est pas toujours évident pour le chef de projet de concilier les contraintes des projets et ses risques.

- La dimension humaine est inévitablement le maillon le plus vulnérable. Par ses erreurs, les négligences et la manque de sensibilisation, elle constitue la principale porte d'entrée pour les cyberattaques.

- Enfin la cybersécurité est désormais un enjeu de gouvernance et de légitimité politique. La protection d'un organisme conditionne la continuité de ses services, la protection des données mais également son image de confiance.

Face à ces constats, le véritable défi n'apparait pas dans les solutions techniques mais bel et bien dans la structure et la gouvernance. Il convient aux organisations d'être capable de traduire ses exigences en procédures opérationnelles adaptées et à développer une culture de sécurité partagée.
La cybersécurité doit être pensée comme un levier stratégique d'efficacité et de résilience organisationnelle.

3.6. Conclusion de la section

Enfin, cette troisième partie a permis de mettre en évidence la fragilité inhérente de la construction des exigences de cybersécurité. En effet, face à une gouvernance encore immature, une dépendance forte aux experts et une traduction opérationnelle complexe, le risque de fragmentation est accru et limite l'appropriation de la part des chefs de projet. Ces constats viennent souligner la nécessité d'outils et de dispositifs d'accompagnement pour rendre la cybersécurité plus accessible. Et pilotable au sein des organisations.

PARTIE 3 – ETUDE DE TERRAIN

Après avoir présenté un cadre théorique et réglementaire ainsi que les principaux enjeux de la cybersécurité intégrée à la gestion de projet, cette troisième partie a pour but de confronter les différents éléments à travers la réalité du terrain. A travers cette partie, mon objectif est de mettre en lumière, par mon expérience, les pratiques effectives et difficultés rencontrées par les chefs de projet pour répondre aux exigences de conformité. Cette étude vise à vérifier mes constats théoriques et identifier les possibles écarts entre les prescriptions et les pratiques afin de proposer par la suite un accompagnement adapté.

1. Démarche de la recherche

L'état de lieux réalisé par mon alternance au sein du Conseil régional d'Île-de-France, appuyé par une analyse détaillée de la littérature à mis en lumière un constat récurrent : La cybersécurité est encore trop peu intégrée dans la pratique de gestion des projets numériques. Malgré la création du Pôle Transformation Numérique pour unifier les pratiques et la présence d'un RSSI et son adjoint dans la DSI, la prise en compte des exigences de sécurité est toujours fragmentée et complexe pour les équipes projets.

Ces chefs de projet se retrouvent donc démunis face à la multiplication des contraintes telles que le RGPD, l'accessibilité, la sécurité des données ou encore l'interopérabilité des données, qui sont trop rarement traduites en procédures opérationnelles claires. Nous faisons alors face à une gouvernance éclatée ou les référentiels méthodologiques sont disparates et la coordination demeure faible.

Ce constat génère des difficultés concrètes mise en exergue par les équipes projets.

L'intégration des exigences en cybersécurité est trop tardive alors que celle-ci nécessiterait une intégration bien en amont du projet. Elle doit être considérée dès la conception du projet. La dépendance aux prestataires externes est très forte et ne permet pas un transfert de compétence vers les agents du conseil régional. Cela induit en conséquence un manque de sensibilisation et de formation pour les chefs de projets et les utilisateurs accentuant ainsi la vulnérabilité humaine mise en avant dans la littérature.

C’est dans ce contexte que nous avons retenu la problématique suivante : Comment piloter efficacement les exigences de cybersécurité dans un contexte organisationnel marqué par le manque de clarté, la fragmentation ou l’absence de procédure strcturée ?

Cette problématique implique de croiser trois dimensions essentielles pour l’approche de résolution l’étude de terrain, qui ont pu être soulevées au cours de la revue de littérature.
La dimension humaine qui s’applique à travers l’étude des comportements, la sensibilisation et les biais cognitifs qui impactent notre sécurité au quotidien.
La dimension organisationnelle pour créer des technique communes et une culture du risque partagée pour une gouvernance plus intégrée.
La dimension stratégique pour affirmer la cybersécurité comme un axe structurant de nos projets et non comme une obligation subie.
Afin d’appuyer ma recherche et mes constats par des témoignages réels et des retours d’expériences, ma méthodologie s’est retenue sur une étude qualitative à travers des interview réalisées au sein du Conseil Régional.
Cette démarche m’a permis de soulever les points essentiels et de traduire la revue de littérature en problématique de terrain réelle.
J’ai également effectué une observation participante, m’ayant permis de comprendre le fonctionnement d’un organisme complexe et de m’imprégner de son mode de fonctionnement.

Les enjeux sont forts au sein d’une collectivité telle que le Conseil régional d’Île de France. Nous évoquons une organisation qui a en charge des milliers de franciliens ainsi que la livraison de services essentiels pour le bon fonctionnement du territoire.
Nous pourrions penser qu’au regard des risques, les moyens pour sécuriser l’environnement sont colossaux et les agents surentrainés. Mais a contrario, les processus comme les agents sont encore bien loin de la sécurité parfaite.
Comme nous avons pu l’évoquer dans le triangle des trois contraintes, les organisations publiques subissent en plus des contraintes de budget. En effet, leurs marges de manœuvre sont souvent limitées par des arbitrages financiers décidés en grandes partie par l’état ou par des décisions politiques, ce qui restreint davantage la mise en œuvre de certains projets numériques.

1.1. La sécurité idéale

Nous avons évoqué dans la revue de littérature quelques notions pour mettre en place la cybersécurité. Mais sur le terrain quels sont les étapes nécessaires et essentielles pour instaurer la sécurité parfaite ? Nous allons décrire le processus idéal à suivre, comme évoqué la plupart du temps dans les documents de référence. Ce processus est essentiel pour assurer la cyber-résilience en entreprise.

Mise en lumière par les auteurs, la cybersécurité doit être vue comme une stratégie globale et intégrée. Pour cela elle doit être pensée et soutenue dans les plus hauts niveaux de gouvernance. La littérature comme les rapports des différents organismes convergent vers un modèle « *Secure by design* » dans laquelle la sécurité est un levier de confiance et de résilience organisationnelle. Dans une approche « *Secure by design* », plusieurs éléments doivent être pris en compte pour la conception du système. Il faut tout d'abord comprendre les menaces auxquels les systèmes sont exposés. Il faut par la suite minimiser la surface d'attaque, cela passe par le fait de restreindre certains accès afin de réduire les points d'entrée. La restriction est faite en fonction des distinctions des privilèges et la définition des rôles.
En externe il faut être vigilant vis-à-vis des services tiers et des prestataires qui peuvent être un point d'entrée aux intrusions.
Cette sécurité by design se traduit cependant par un processus clair et défini et le respect de plusieurs étapes nécessaires à son implémentation.

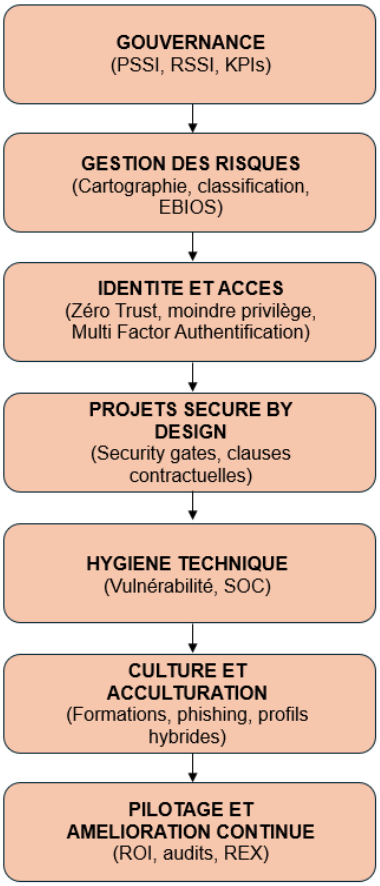

Figure 12 : Security by design (personnel)

La première étape s'inscrit via une gouvernance claire et soutenue par la hiérarchie.

La première condition pour la réussite d'une cybersécurité efficace réside dans l'encrage stratégique fort. Cela suppose que le RSSI dispose de mandats explicites, d'une certaine légitimité et de ressources nécessaires à la sécurité. Dans cette approche la PSSI (politique de sécurité des systèmes d'information) constitue le document de référence pour les obligations réglementaires. Elle doit être, en théorie, lue et assimilée par tous les employés concernés par la gestion numérique.

Une gouvernance idéale repose également sur un RACI explicite, en cours de construction au Conseil régional. Celui-ci permettrait de clarifier les rôles des métiers ainsi que tous les secteurs de l'IT, du juridique ou encore du RSSI.

Et enfin, il doit exister un tableau de bord qui fournit l'indicateur concret en termes de délais, de taux de conformité, en couverture ou en taux d'expositions critiques.

Par la suite l'approche doit être structurée par la gestion des risques. Les organisations doivent adopter une démarche systémique de gestion des risques. Cela commence notamment par la cartographie des actifs accompagnée d'une classification claire des informations selon leurs sensibilité. Des analyses de risques doivent être menées de manière régulière à l'aide de méthodes connues telles que EBIOS. Ces analyses permettent de prendre en compte l'environnement interne tout autant que l'environnement externe lié aux prestataires et aux chaines d'approvisionnement.

La méthode EBIOS se traduit par une approche de management du risque numérique en passant par tous les niveaux, du plus haut, jusqu'aux fonctions métiers. Elle vise à étudier les différents scénarios de risques possibles par des ateliers, comme illustrés dans la figure ci-dessous. L'objectif est ainsi de développer des plans de traitement des risques avec les mesures préventives et les mesures compensatoires.

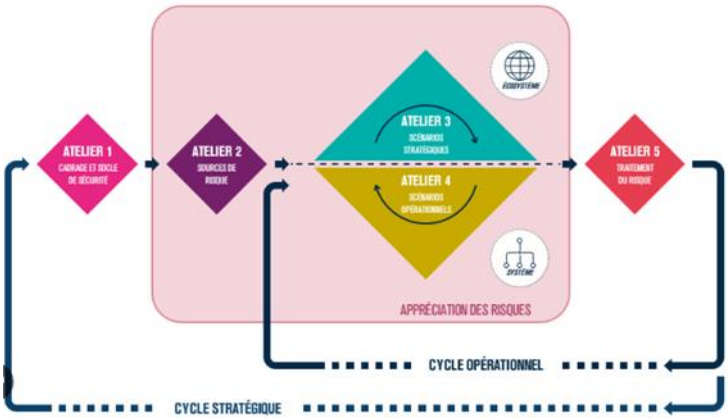

Figure 13 : Méthode EBIOS, démarche itérative (ANSSI)

La sécurité passe nécessairement par la gestion des identités et des accès selon le modèle « Zero Trust ».

Aujourd'hui, il est de mise de remettre en cause le modèle classique et d'instaurer un modèle plus strict mais plus sécuritaire. Cela se traduit par l'application du moindre privilège en accordant uniquement les droits strictement nécessaires à chaque individu selon ses missions. Les authentifications fortes sont nécessaires ainsi qu'une bonne gestion des identités et des habilitations intégrées aux cycles de vie des employés. Et enfin, l'idéal est d'offrir un réseau d'administration séparé pour protéger les comptes sensibles conformément aux réglementations de l'ANSSI ainsi qu'aux exigences de NIS2.

La prochaine étape impose l'intégration de la sécurité dans les projets et produits numériques. La stratégie idéale nécessite une sécurité intégrée en amont du cycle de vie des projets et un accompagnement des chefs de projet par des outils méthodologies clairs. Parallèlement des étapes de sécurité doivent être réalisées « security gates » afin de valider les architectures et effectuer des tests et audits pour les projets critiques. Enfin, les clauses contractuelles de cybersécurité doivent être systématiques dans les marchés publics comme privés.

Une organisation se doit de garder une hygiène technique et opérationnelle forte. En effet la prévention et la détection reposent sur un socle technique robuste. Cela permet la gestion proactive des vulnérabilités, une surveillance continue et un plan de résilience constitué d'exercices.
En parallèle de ces outils techniques, la culture organisationnelle est tout aussi importante. Une stratégie idéale ne peut pas aboutir sans une dimension humaine forte. Chaque équipe, en fonction de ses missions, doit bénéficier de formations différenciées et adaptées à leurs rôles. La sécurité devrait ainsi être intégrée dans les objectifs de performance des manageurs. Et enfin il serait pertinent d'instaurer des profils hybrides formés sur les bases de la cybersécurité et son pilotage. C'est un moyen efficace de traduire les exigences en langage opérationnel.

Pour finir les étapes nécessaires à une bonne cybersécurité, il est essentiel de conclure par un pilotage pragmatique basé sur l'amélioration continue. Les mesures doivent être abritées selon leurs cout et leur réduction de risques afin d'optimiser les budgets et éviter l'installation d'outils multiples. Les tests et incidents doivent être nourris de retours d'expérience systématiques ainsi que des ajustements en cas de nécessité. Et enfin des audits de manière régulière permettent de tester la robustesse des dispositifs et ainsi d'aligner la stratégie en phase avec les évolutions réglementaires et les technologies.
Les grandes instances mettent en avant ces plans de cyber-résilience pour les entreprises comme illustré sur le document suivant. Les étapes sont distinguées et clairement évoquées dans les plans d'actions.
Cependant nous allons désormais faire un focus sur l'état réel de la cybersécurité dans les organisations d'aujourd'hui.

Figure 14 : Piloter la cybersécurité (cybermalveillance.gouv)

1.2. Situation réelle

Si la littérature et les grandes instances s'accordent sur les principes d'une cybersécurité intégrée et gouvernée, la réalité des organisations montre que cette maturité est loin d'être une réalité. Plusieurs enquêtes et rapports mettent en évidence les écarts qui persistent sur les points essentiels tels que la gouvernance, l'acculturation, les ressources et les capacités techniques. Nous verrons par la suite que les entretiens réalisés dans le cadre de mon mémoire confirment ce constat.

La maturité globale en termes de cybersécurité reste stagnante. En effet les études récentes évoquent un ralentissement de la progression en maturité cyber. Dans son étude le « *Cyber Benchmark 2025* », *Wavestone* estime la maturité moyenne des grandes entreprises à 54%. Une très faible progression par rapport à 2024 qui traduit l'atteinte d'un pallier structurel. Ce constat affirme l'utilité urgente de réformes organisationnelles profondes et d'investissements durables pour franchir ce pallier. Dans un même temps le *World Economic Forum* met en avant dans son « *Global Cybersecurity Outlook 2025* », la complexité croissante des cybermenaces face à la pénurie des compétences. En effet, un fait alarmant est énoncé : le manque de main d'œuvre en cybersécurité s'est accru de 8% en un an et au moins deux tiers des organisations déclarent souffrir de lacunes modérées en termes de compétences. Selon l'entreprise Accenture en 2025, seulement une organisation sur 10 se dit prête à faire face aux menaces cyber augmentée par l'IA. 63% seraient dans une « *Exposed Zone* » ce qui signifie un manque cruel de stratégie cohérente et des capacités techniques insuffisantes. L'IA ouvre la voie à de nouvelles innovations, mais celles-ci ne seront pas forcément bénéfiques. En effet les risques et menaces liés à son usage offrent également de nouvelles opportunités d'exploitation.

Les chiffres confirment que la dimension humaine est un élément central dans les failles et erreurs de sécurité. *Le Verizon Data Breach Investigations Report 2025* annonce qu'environ 60% des incidents de sécurité sont causés par l'humain qu'il puisse s'agir d'erreurs, d'ingénierie sociale ou de mauvaise gestion des droits.

En plus de ces démonstrations, des études font part de coûts et délais de réponse préoccupants. En effet un écart important entre l'idéal et la pratique se traduit par des coûts élevés ainsi qu'une réactivité trop faible. Le rapport IBM 2025 Cost of a Data Breach estime que le cout moyen d'une violation de donnée est de 4,4 millions de dollars au niveau mondial. En plus de cela les délais moyens pour que les brèches soient identifiées et contenues est de 276 jours soit environ 9 mois.

La cybersécurité souffre également d'un risque majeur trop peu remonté : la dépendance aux fournisseurs et prestataires. L'étude *Kiteworks* de 2025 montre que les organisations travaillant avec plus de 1000 prestataires connaissent en moyenne sept brèches par an liées à leur *supply chain*. Par ailleurs, la prolifération d'outils et de systèmes d'informations crée une forte complexité qui est, à long terme, contre-productive. Certaines entreprises utilisent aujourd'hui plus de 80 solutions de sécurité en simultané qui en réalité augmente les délais de détection des réponses aux incidents.

Pour faire face aux nombreuses menaces, les obligations règlementaires se multiplient. Bien qu'elles aient une volonté structurante elles ne sont pas encore pleinement respectées. En effet la directive NIS 2 a élargi considérablement le périmètre des entités soumises.

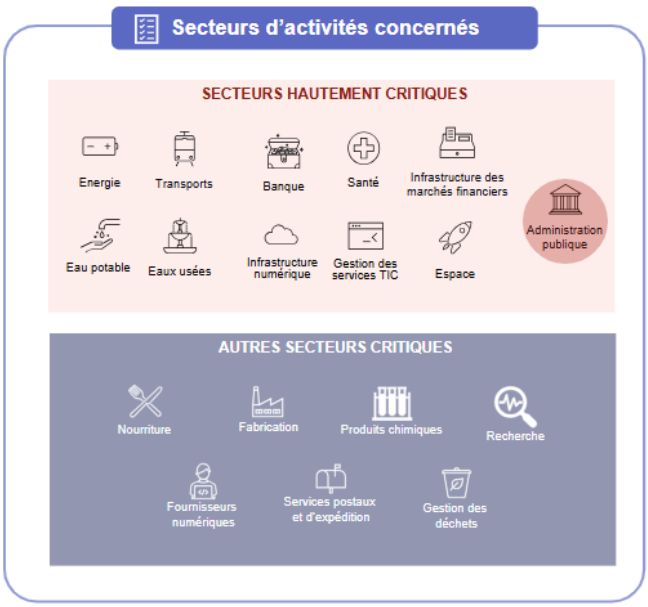

Figure 15 : Secteurs d'activités concernés par la NIS 2 (Région Île-de-France)

Cette nouvelle gouvernance impose des exigences de gouvernance, de détection, de résilience et de reporting sous 24heures.
Or en dépit de l'intention de cette nouvelle directive, plusieurs collectivités et entreprises témoignent de difficultés pour la mise en conformité.

Nous allons désormais mettre en perspective ces constats à travers mon étude de terrain à la région Île-de-France.

2. Etude de terrain empirique

Dans le prolongement des observations menées, j'ai pu conduire une série d'entretiens semi-directifs avec différents acteurs impliqués dans les exigences de sécurité tels que des chefs de projet, un RSSI, des référents RGPD ou encore des consultants externes. Ces échanges ont donc été conduit dans le but de recueillir les perceptions et difficultés ressenties face aux exigences de sécurité. Ces témoignages récoltés constituent pour mon étude une source précieuse pour comprendre la réalité du terrain et me permet d'illustrer concrètement les enjeux de fragmentation et de manque de clarté des exigences au sein de l'organisation.

2.1. Le point de vue des prestataires

Parmi les entretiens réalisés, j'ai pu échanger avec deux consultantes en cybersécurité intervenant au sein du Conseil régional, dont la mission portait sur l'implémentation opérationnelle de la feuille de route NIS2. Cet entretien m'a offert une perspective externe sur la Région Île-de-France à travers le regard de deux consultantes en interaction directe avec les chefs de projet et confrontées aux problématiques de terrain des différentes équipes.

Tout d'abord il est souligné d'emblée que le mise en conformité NIS2 est un processus long et progressif. Il est illusoire de penser qu'une stratégie s'implémente immédiatement. Il faut donc intégrer ces changements dans une temporalité pluriannuelle. « *[…] on établit la feuille de route qui va permettre à la Région d'être en conformité. Donc, la Région, elle ne sera pas conforme immédiatement mais dans 3 ans. C'est la cible.* » Cela souligne l'importance d'un pilotage stratégique avec des jalons clairs afin de répartir l'effort sur la durée.

Par ailleurs, l'un des points insistant dans cet entretien s'est porté sur la place des chefs de projet numériques qui sont des relais essentiels de la conformité. En effet la nouvelle directive impose une actualisation des référentiels et des pratiques à chaque phase des projets. *« […] et donc c'est là ou on va s'appuyer notamment sur ces chefs de projets dans le cas d'intégration de la sécurité dans les projets […]. Il y a pleins de choses sur lesquelles ils vont pouvoir aller chercher des actions de mises en conformité à court terme* ».

Cette implémentation de NIS2 dépend donc aussi bien des experts que de la capacité d'acculturation et d'appropriation par les équipes projets. En effet, la directive introduit des

mesures qui nécessitent des investissements lourds ainsi que du temps de mise en œuvre. L'anticipation est ainsi également un impératif stratégique. Sans anticipation les risques de blocages opérationnels sont plus importants. *« […] c'est tout de même important pour la région d'anticiper ce travail parce qu'il y a des actions qui pourraient prendre plus de temps et plus du budget, qui auraient plus d'enjeux.* »

Le constat de maturité organisationnelle limitée est visible et les ressources contraignent fortement les collectivités. Il est souligné que sans moyens humains, la gestion efficace des risques et la documentation ne peuvent pas être intégrés de manière systématique. « *[…] quand tu as des petites équipes, parce que justement petite maturité ou peu de budget, tu peux difficilement dédier un temps plein à l'organisation ou au suivi et à la réunion de ces indices de risques, ces outils de conformité, etc.* » Ces contraintes de ressources limitent ainsi les capacités des collectivités à répondre aux exigences et notamment en termes de résilience. Et si NIS 2 offre un cadre structurant, certaines dispositions sont difficiles à traduire de manière opérationnelle pour les acteurs de terrain. Il est alors essentiel de disposer d'une certaine connaissance du contexte. « *Pour adresser NIS 2, et sans faire une interprétation, il faut une certaine expérience et une connaissance du terrain qui est importante. Déjà, il y a certaines mesures qui sont un peu, à mon sens, un peu floues*. »

Au-delà des infrastructures techniques, la réussite de la conformité repose sur l'acculturation des chefs de projet. En effet, il est nécessaire de revoir et adapter les pratiques de gestion de projet pour intégrer de manière proactive la sécurité. *« Il y a un travail d'acculturation de la sécurité pour rendre aussi actifs les chefs de projet. […] C'est un mix entre la sensibilisation de fond et ce fameux process d'intégration de la sécurité dans les projets qui est à revoir, ajuster et même peut-être repenser* ». Mettre en place des outils concrets tels que des boites à outils ou des checklists seraient de bons leviers opérationnels pour faciliter l'appropriation. « *[…] la cible est, tu as raison, c'est une boite à outils pour que demain le chef de projet il soit conscient à minima de l'approche par les risques parce que c'est ce qui est le plus facile à expliquer* ».

Enfin l'entretien souligne que certains chefs de projet, notamment ceux de l'IT peuvent être réticents à l'idée d'intégrer la sécurité dans leur périmètre, le considérant comme annexe à leur métier. « *[…] ça va être les chefs de projet IT qui disent : « c'est bon, IT, c'est mon métier ». Mais ils ne sont pas spécialisés* ». Ce cloisonnement organisationnel bloque la transversalité et influe le risque de dérive de la part des équipes. Un problème récurrent est l'accumulation des droits d'accès non-révisés. Cela s'explique souvent par l'absence de processus systématique qui ne surveillent donc pas les points d'accès. « *[…] par exemple, Marc travaillait avant dans*

un autre service et en bougeant de service, on n'a pas revu ses droits d'accès, parce que c'est IT et c'est très confortable d'accumuler ses droits ».

Pour finir, les consultantes interviewées ont rappelé que la sécurité ne doit pas être perçue comme un frein aux projets. Cependant, force est de constater que les arbitrages restent difficiles notamment dans certains secteurs qui sont orientés vers la performance économique. « *Dans le secteur du luxe, la sécurité n'avait pas vocation à bloquer les mises en production […] mais il arrive que des projets soient mené sans la sécurité et qu'on frappe à la porte au dernier moment pour valider* ». Dans ce contexte la mise en place de clauses contractuelles et des mécanismes d'audit envers les prestataires sont bien utiles mais ne remplace pas une intégration de la sécurité en amont du projet.

Cette enquête de terrain auprès des prestataires met en lumière une forte complexité et notamment pour la mise en conformité de NIS 2 au sein d'une grande collectivité territoriale. Cet entretien confirme la nécessité d'une planification à long terme ainsi qu'une acculturation progressive des équipes et un accompagnement opérationnel face aux exigences qui peuvent être difficiles à interpréter. Seule une démarche progressive et outillée peut contribuer à surmonter ces freins.

2.2. La vision interne

Cette perspective externe est précieuse car elle permet d'appréhender la manière dont l'organisation est perçue de l'extérieur et d'avoir un témoignage de personnes travaillant dans plusieurs organisations. Toutefois il demeure essentiel de compléter cette approche avec des témoignages d'acteurs directement confrontés aux enjeux perçus au cœur même de l'activité.

Mon travail s'est donc porté autour de plusieurs postes et fonctions différentes afin d'obtenir une vision large et spécifique du sujet.

Mes entretiens se sont déroulés autour de plusieurs thématiques centrales récurrentes. La première portait sur la perception des exigences avec le type de question « Quelles sont les exigences les plus difficiles à intégrer dans les projets selon vous ? ».

La seconde thématique portait sur les modalités de mise en œuvre des exigences de cybersécurité notamment à travers le recueil de témoignage et de retours d'expérience des individus concernés.

La troisième thématique s'attachait à analyser les actions entreprises par l'organisation face à la complexité des exigences.
Enfin, l'entretien se clôturait par la collecte des préconisation et recommandations formulées par les parties prenantes interrogées.

2.2.1. La responsabilité limitée des chefs de projet

L'un des principaux constat émis à la suite de mon entretien résulte dans la dépendance structurelle des chefs de projets vis-à-vis des experts sécurité et techniques. Face aux exigences perçues comme trop techniques, complexes ou spécialisées, ils vont déléguer les décisions aux référents ou au RSSI. Plusieurs chefs de projets l'expliquent dans leur témoignage : « *Si j'ai un doute en termes d'infra ou de réseau je vais penser à […] je préfère m'appuyer sur les ressources internes quitte à ce que, eux prennent la décision et pas moi en tant que chef de projet* ». Par ailleurs ce constat est souligné par un autre chef de projet numérique lorsque je pose la question : « *Est-ce que tu trouves que les exigences de cybersécurité sont compréhensibles dans tes projets ?* ». La réponse est « *Je n'en ai pas connaissance. Je vais me reposer sur le RSSI et son expertise. Je vais m'appuyer sur les experts* ». Cette posture est très largement explicable. En effet dans un environnement ou les normes évoluent très rapidement et ou les enjeux techniques dépassent les compétences généralistes, les chefs de projets n'ont d'autres choix que de se tourner vers les experts. Néanmoins cela révèle la faible autonomie des chefs de projets qui retrouvent parfois dans un rôle d'intermédiaires. Sans méthodologie claire ou de checklist, leur marge d'action est limitée. L'illisibilité des processus empêche les acteurs de première ligne d'exécuter les exigences.

2.2.2. Le manque de communication et tensions organisationnelles

En dehors des aspects techniques et des compétences, les entretiens ont mis en exergue une certaine tension entre métiers et techniques. Cette fracture influe sur la coopération et vient alourdir les cycles des projets. Un chef de projet le souligne :« *On va dire une petite guéguerre entre les chefs de projet applicatifs et les services plus techniques qui eux sont dans leur monde […]. Parfois ils n'entendent pas trop ça.* » Cela illustre la distance culturelle et fonctionnelle entre les différentes équipes. En effet, les équipes techniques vont se concentrer sur la

robustesse et la sécurité lorsque les métiers ont des impératifs à respecter vis-à-vis des relations avec les éditeurs ou les utilisateurs finaux. Les chefs de projets se retrouvent parfois à devoir arbitrer des logiques contradictoires.

A cela s'ajoute une grande lacune au sein du Conseil régional qui est le problème récurrent de communication insuffisante. Certains chefs de projet évoquent l'absence de retours de la part du RSSI : « *Le RSSI m'a demandé de produire un document dans le cadre d'un projet, je n'ai jamais eu de retour dessus après plusieurs relances.* » La manque de retour et de feedback fragilise la confiance et accentue un sentiment que la cybersécurité est une contrainte externe plutôt qu'un processus intégré.

2.2.3. Une sensibilisation présente mais fragmentée

Les entretiens montrent néanmoins que les équipes ont acquis une culture de base de la cybersécurité et en particulier sur la protection des données personnelles. Désormais les chefs de projet savent identifier une donnée sensible et comprennent l'importance des risques. La référente RGPD du pôle transformation numérique note : *« Ils savent ce qu'est une donnée personnelle, ils savent quand c'est sensible, ils savent qu'il faut des durées de conservation […]. Après ce qui va être compliqué, ça va être de détecter que c'est une violation de données.* » ;« *[…] Oui, j'ai constaté deux choses. Leur prise de connaissance, de conscience, tu vois que c'est une donnée personnelle : alerte rouge. Et sur les questions qui nous sont posées, elles sont vraiment de plus en plus pointues*."

Cependant malgré la prise de conscience des enjeux amenée par les référents, l'acculturation reste incomplète et inégale. Les chefs de projet, eux, évoquent un apprentissage « sur le tas » avec peu de formations structurées. « *[…] pas vraiment de formations j'apprends sur le tas […]. Une sensibilisation à la cybersécurité l'année dernière, mais pas de formation NIS2 ou autre.* » Cela traduit un effort de sensibilisation mais non systématique. L'un ajoute : « *Je pense qu'il faut un peu plus de transparence au sein de la DSI sur ces aspects-là, sur les enjeux de cybersécurité. De toute façon, la transparence, la communication, c'est le b.a.-ba de la prévention sécurité* »

Le besoin de supports simples et régulier est revenu chez plusieurs interlocuteurs : « *ça aurait été bien qu'on ait un kit simplifié […] ou même des mails trimestriels de veille envoyés par les référents […] les lois évoluent enfin la cybersécurité évolue. Donc comme je t'ai dit, si on a un*

kit simplifié, très bien pour moi. » Cette demande d'outils concret pour aider les chefs de projet montre que la sensibilisation ne peut pas se limiter à des actions ponctuelles mais doit être institutionnalisée. « *[…] tout est utile. Une documentation est utile, si elle est, et peut être lue* »

2.2.4. Le manque de processus intégrés

Un des autres freins identifiés concerne les processus organisationnels mal connus ou fragmentés. Les chefs de projet savent que les obligations existent mais n'ont pas de cadre et de référentiel pour les appliquer concrètement. Un référent explique : « *Je ne pense pas que ce soit une confusion sur les lois, mais plus en termes de process […] C'est une mauvaise connaissance des process […] on n'a pas de document unique. Du coup la personne vient pour le RGPD et on lui dit : est-ce que tu as fait ci ? est-ce que tu as fait ça ?* ». Ce constat est renforcé par le témoignage de chefs de projets : « *Il manque quand même la mise en place de de procédures et de process*. » En effet cette absence de référentiel transversal engendre des redondances, des oublis ou accroit la complexité. Chaque exigence est traitée de façon séparée dans une vision globale sécurisée. C'est ainsi que découle la fragmentation organisationnelle ou les silos persistent.

2.2.5. Une gouvernance peu lisible

Comme évoqué précédemment, le besoin d'un processus unifié et lisible est un élément remonté dans presque tous les entretiens. Ce processus permettrait de guider les chefs de projets dans leurs démarches. Actuellement, ceux-ci naviguent tous entre le RSSI ou les référents RGPD, accessibilité, open Data…Ils ne savent pas clairement qui solliciter et à quel moment. Un référent explique donc le besoin : « *Il faut un process global où on dit : ça c'est RSSI, ça c'est open data, ça c'est accessibilité, ça c'est RGPD*. » Avec l'absence d'un document unique, les acteurs doivent s'appuyer sur leurs réseaux informels et leurs connaissances personnelles mais qui peuvent créer des inégalités. Les plus anciens et expérimentés savent à qui s'adresser mais les plus récents se retrouvent en difficulté. « *[…] je fais la démarche d'aller voir les gens […] ça fait longtemps que je suis à la DSI et ça aide. C'est plus facile de connaitre les gens, je sais où aller.* » Cette situation peut provoquer une pression et une surcharge sur les référents souvent sollicités de très nombreuses fois : « *[…] ils s'appuient énormément sur leurs référents*

sans comprendre que le référent n'est pas extra-lucide […]. Ils demandent : faites-moi la clause, alors qu'on ne peut pas deviner leur besoin. »
Une gouvernance claire et structurée permettrait de réduire ces dépendances aux référents et experts et de fluidifier la gestion des exigences.

2.2.6. Le pacte de confiance

Enfin, les entretiens nous révèlent une dimension plus éthique et citoyenne de la cybersécurité. Pour plusieurs acteurs, il ne relève pas uniquement de conformité réglementaire mais la région est dotée d'un pacte de confiance avec les usagers. Un référent insiste : « *À la région, on a ce sens de la mission d'intérêt public*. » Une autre ajoute : « *Pour moi ce n'est pas la sanction CNIL la plus grave, c'est la sanction d'image […]. Ce sont des usagers qui s'interrogent et qui ont peur sur ce qu'on fait de leurs données*. » Cette vision confère à la notion de cybersécurité une dimension sociétale et politique. Cela dépasse les aspects techniques et traduit l'importance d'un pilotage rigoureux pour préserver la donnée et la confiance des citoyens.

Cette étude de terrain fait donc apparaitre une situation contrastée au sein du conseil. Les chefs de projet et les équipes montrent une bonne acculturation de base et une bonne conscience aux enjeux de sécurité. Néanmoins ils restent dépendants aux experts pour les aspects techniques trop complexes pour eux.
Il y a un gros manque de processus qui sont fragmentés et sans cadre et procédures consolidées. La cybersécurité est ainsi perçue à la fois comme un obstacle opérationnel mais aussi comme une base de confiance essentielle pour l'organisation.

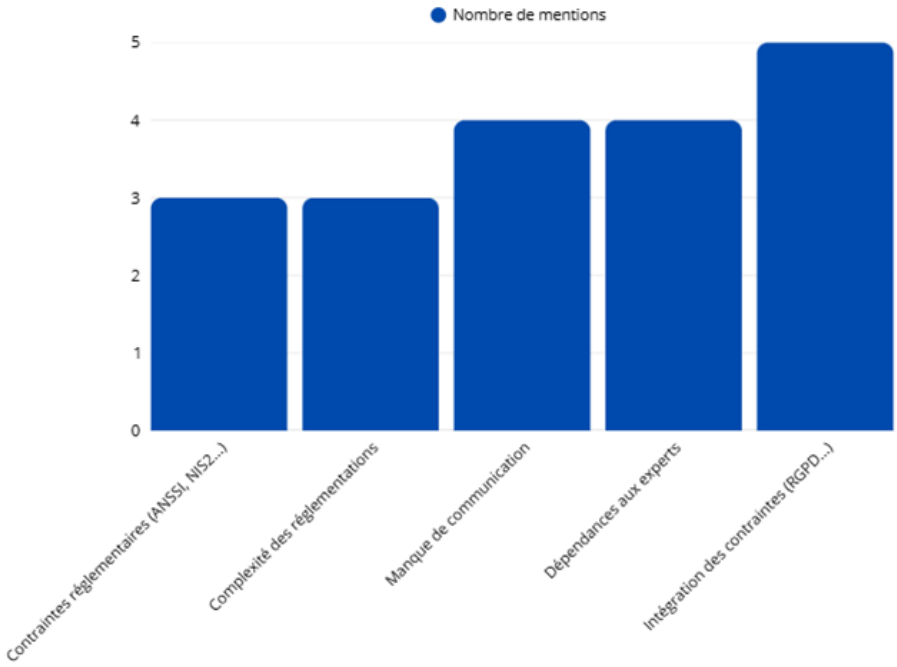

Figure 16 : Mentions récurrentes dans les obstacles à la cybersécurité (personnel)

Ce schéma illustre les points récurrents et le nombre de mentions souvent relevées de certains obstacles identifiés à l'intégration de la cybersécurité.

2.2.7. Le rôle du RSSI

Dans le cadre d'un entretien plus ciblé, j'ai eu l'opportunité d'échanger avec le RSSI de la DSI, intégré au pôle transformation numérique, afin de mieux comprendre la manière dont les procédures sont mises en œuvre concrètement à travers un acteur central de la cybersécurité. Son témoignage met en avant une approche à la fois structurée mais contrainte, poussée par une gestion continue des risques mais aussi par des limites organisationnelles et réglementaires.

Le RSSI décrit ainsi sa mission comme une responsabilité transverse centrale. Elle concerne l'ensemble des projets informatiques industriels et numériques. Il insiste en expliquant : « […] *n'importe quel projet informatique doit respecter certaines exigences.* », qui doivent être reliées à l'APSSI. [7] Dans cette logique, la cybersécurité est une condition préalable à tout déploiement. Il insiste ainsi sur la nécessité de qualifier chaque projet afin de déterminer les niveaux de

[7] *Spécialistes en solutions informatiques*

criticité, ce qui va permettre de fixer les exigences. Cette étape conditionne la suite du travail avec les chefs de projet qui doivent intégrer la sécurité dès la phase de production du projet.

L'une des démarches majeures du RSSI repose également sur la gestion continue des risques. Chaque projet implique une évaluation des risques qu'il soit lié aux infrastructures ou aux usages. « *Normalement pour chaque projet, des Excels sont faits pour respecter les exigences* ». Ces documents constituent un moyen de traçabilité indispensable pour intégrer les exigences de cybersécurité, RGPD et qualité. Le RSSI souligne par ailleurs que dans le domaine informatique, les risques sont presque toujours liés à la cyber. En effet la frontière entre risque IT et cybersécurité est très fine. L'analyse de risque est ainsi un outil indispensable qui permet de qualifier les menaces, d'estimer les impacts et de décider les mesures à mettre en œuvre.
Par la suite, il insiste sur le caractère normé de la cybersécurité. Cela implique de se conformer à des référentiels multiples tels que le RGPD, les normes de qualité ou encore les directives européennes. Cependant il reconnait la difficulté à « connecter les données » et à produire une vision consolidée des données.
L'un des points centraux évoqué concernait la directive NIS 2. Le RSSI observe que la France a pris du retard sur son implémentation, les entreprises n'ayant pas entrepris les investissements nécessaires. Alors que « *beaucoup de groupes sont déjà compliant* », les acteurs publics comme la Région doivent encore « *éplucher NIS 2* » pour démontrer leur conformité. L'objectif est clair : atteindre un niveau de conformité mais les moyens et les méthodes sont à consolider. Cela illustre bien le décalage persistant entre les ambitions réglementaires et la capacité opérationnelle à les mettre en œuvre.
Par la suite le RSSI reconnaît que dans la pratique, l'analyse de risques guide les projets, mais la norme n'est jamais le moteur principal. C'est-à-dire que les équipes vont dans un premier temps aller sur l'opérationnel et ensuite seulement, chercher à aligner les pratiques avec les référentiels. Cette pratique a le mérite de faire avancer mais elle génère un véritable « *gruyère organisationnel* » engendrant de multiples trous et incohérences dans l'application des exigences.
Aujourd'hui le Conseil régional d'Île de France a atteint un certain niveau de maturité réglementaire mais celle-ci n'est pas en mesure de « *faire une réévaluation de l'analyse de risque* » ni de construire « *une base centralisée sur les normes des projets pour voir l'évolution.* » Pour conclure cet échange il appuie sur la multiplication des réglementations auxquelles la Région est soumise : NIS 1 étendue à NIS 2, la loi de programmation militaire, le

Cyber Résilience Act[8], et d'autres encore. Cette inflation normative devrait amener une cartographie claire des obligations mais aujourd'hui aucun dispositif unifié n'a été mis en place.

2.3. Conclusion des entretiens

L'analyse des entretiens menés auprès des chefs de projet, référents, RSSI et consultantes externes met en lumière une réalité contrastée. D'un côté, nous apercevons une sensibilisation croissante et une prise de conscience de l'importance de la cybersécurité ; de l'autre, il demeure un manque de lisibilité des processus, une dépendance forte aux experts, et une gouvernance encore fragmentée. La cybersécurité est reconnue en théorie comme essentielle mais reste trop peu lisible pour les chefs de projet.

Les processus sont fragmentés et la communication inefficace ou insuffisante pour la gestion des projets complexes.

La sensibilisation existe, elle considérée comme essentielle et fortement utile. Cependant sans véritable programme et formation structurées, le souhait de sensibiliser n'est pas suffisant. Il faut inculquer aux acteurs les vrais dangers de la cybersécurité et marquer les esprits par des messages et avertissements clairs.

Enfin le RSSI joue un rôle clé mais reste également limité par le manque d'outillage consolidé.

La région est sujet à un pacte de confiance avec ses citoyens et se doit de respecter ses engagements à respecter leurs données et leur intégrité.

Ces résultats confirment la problématique centrale du mémoire : l'illisibilité et le manque de structuration des exigences de cybersécurité pour les chefs de projet constituent un frein majeur à leur intégration dans les projets numériques.

[8] *Renforce les normes de cybersécurité des produits qui contiennent un composant numérique, exigeant des fabricants et des détaillants qu'ils garantissent la cybersécurité tout au long du cycle de vie de leurs produits.*

PARTIE 4 – APPROCHE DE RESOLUTION

Afin de répondre à ces différentes problématiques énoncées je propose deux étapes de résolutions. Dans un premier temps je vais présenter un modèle de kit établi dans le but d'accompagner et d'offrir un référentiel pour les chefs de projets. Celui-ci aborde les sujets de sécurité (cybersécurité et RGPD) et aurait pour but d'être étendu à toutes les exigences de la Région Île-de-France (accessibilité, open data, urbanisation, archivage…) afin d'en faire un guide unique pratique pour les chefs de projets.
Dans un seconds je développerai des recommandations dans le but de répondre aux problématiques et d'accompagner le Conseil régional à pallier les manquements observés.

1. Proposition d'un Kit à destination des chefs de projet

Le support qui suit a été établi dans l'optique de proposer un processus structuré et clair pour les chefs de projets. Nous allons expliquer les différentes étapes ainsi que les informations liées à ce support.

Le schéma présenté est une proposition de check-list de cybersécurité et conformité RGPD. Elle est organisée selon le cycle de vie d'un projet numérique.
Ce support a pour but de répondre directement aux constats formulés dans les différents échanges : le manque de clarté des processus, la dépendance aux experts et l'absence de guide pratique pour les chefs de projet. L'objectif est ainsi de fournir un outil, concret, facile d'utilisation qui garantit l'intégration des exigences essentielles liées à la sécurité et à la conformité.

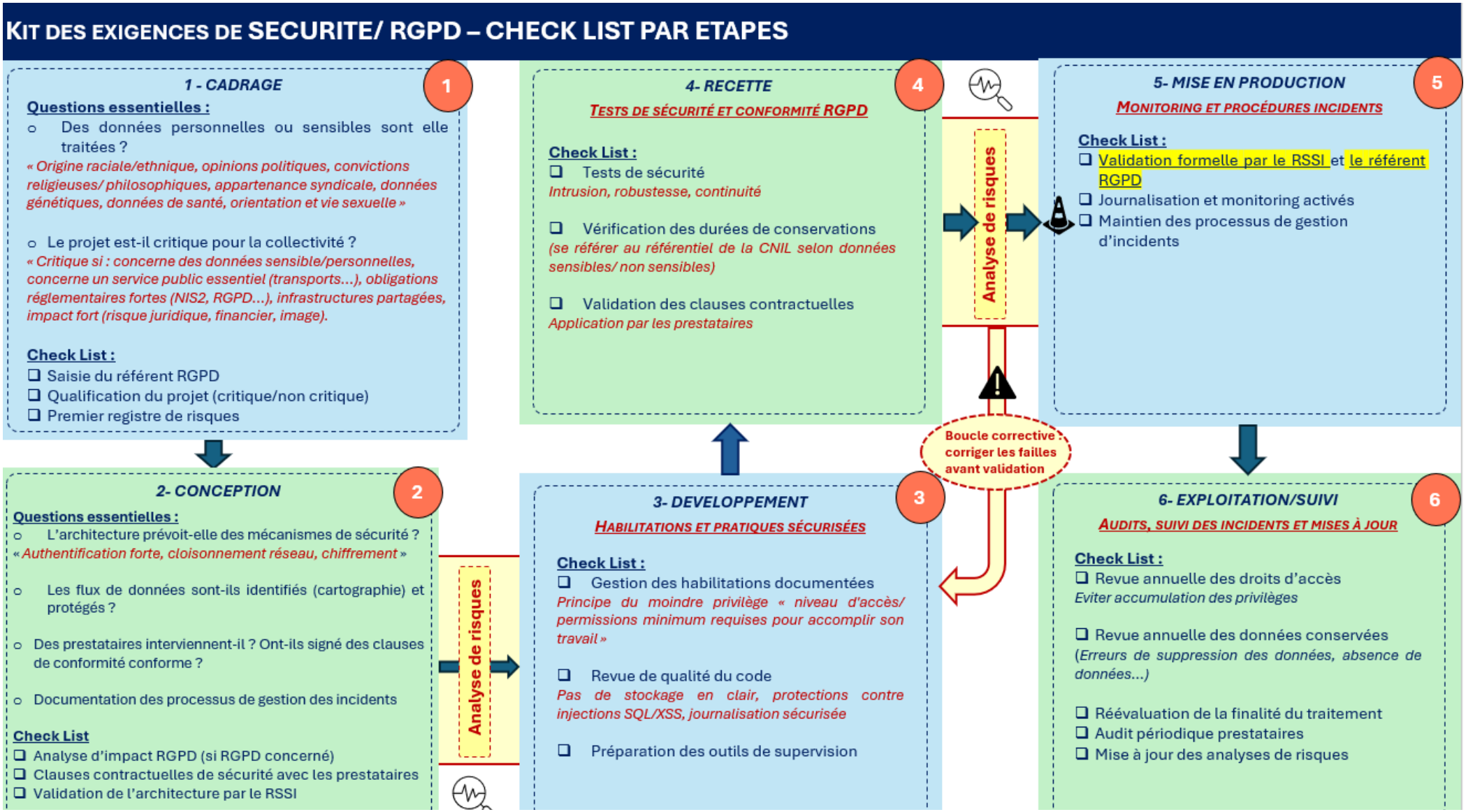

Figure 17 : Kit des exigences de sécurité/RGPD (personnel)

1.1. Cadrage

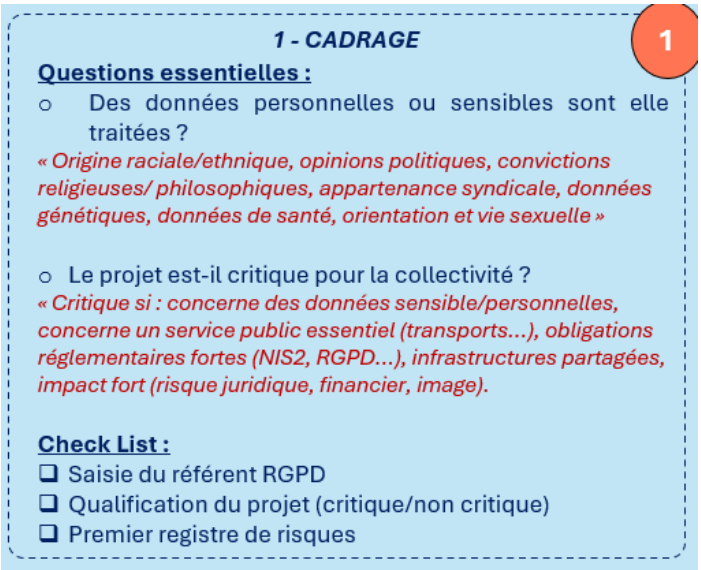

Figure 18 : Kit des exigences de sécurité/RGPD - Cadrage (personnel)

Le cadrage est le point de départ stratégique du projet. Il permet la qualification du projet avant tout engagement. Dans une organisation telle que la Région Île-de-France, où les projets sont multiples, cette étape est indispensable et va ainsi distinguer les projets critiques du reste des projets. Elle va ainsi poser les bases en matière de sécurité et de conformité RGPD en apportant une grille de lecture aux chefs de projet.

Il convient de se poser des questions essentielles sur plusieurs points :

- La nature des données traitées : est-ce que le projet a pour but de manipuler des données personnelles (noms, adresses, email, dossiers d'usagers…) ou des données sensibles au sens du RGPD (Origine raciale, opinions politiques, données de santé…)

  Ce premier passage est déterminant car il permet de déclencher les obligations spécifiques telle que l'analyse d'impact RGPD.
- La criticité pour la collectivité : est-ce que le projet concerne un service public essentiel comme les transports, les aides sociales ou l'éducation ? Est-ce que celui-ci est soumis à des cadres réglementaires stricts ? (NIS 2, RGPD, RGS[9]…) Ou encore, le projet

[9] *Le référentiel général de sécurité (vise à limiter la fraude liée à l'usage des services numériques de l'Administration.)*

impacte-t-il des infrastructures partagées entre plusieurs services ou collectivités ? Et enfin, si une faille devait apparaitre quel serait l'impact sur l'organisation ? (Juridique, financier, réputationnel…)

Cela va permettre d'identifier tous les risques majeurs dès l'amorçage et permet la première construction du registre de risques.

A l'issu de ce cadrage, plusieurs livrables sont attendus :

- Qualification du niveau de sensibilité via le questionnaire permettant de qualifier la nature des données et leur niveau de criticité, en ayant préalablement saisi le référent RGPD dès le départ.
- Le registre initial des risques qui est une première version, enrichie et actualisée tout le long du projet.
- La qualification de la criticité du projet qui est une décision formalisée par le RSSI et le référent RGPD. Celui-ci permet d'ajuster les exigences dans les étapes suivantes.

La phase de cadrage est bien évidemment un travail collaboratif qui nécessite l'intervention du référent RGPD et du RSSI pour une expertise sécurisée et une qualification valide.

En proposant une étape de cadrage structurée avec des check-list cela permet de combler le manque de socle méthodologique commun.

1.2. Conception

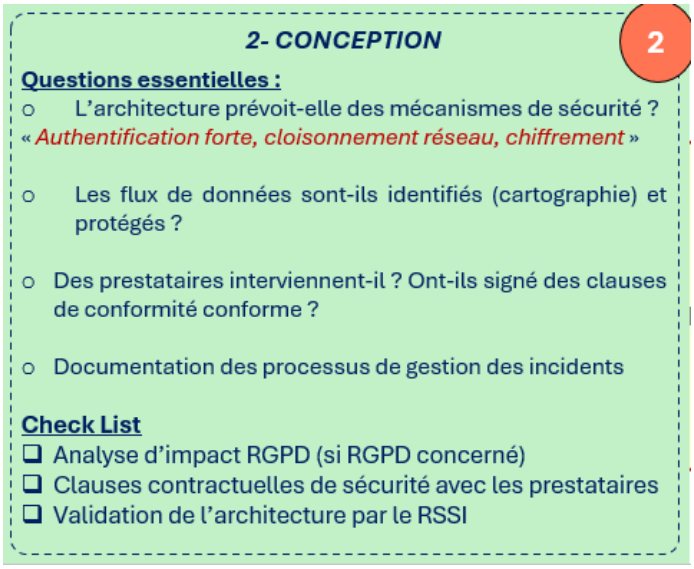

Figure 19 : Kit des exigences de sécurité/RGPD - Conception (personnel)

La phase de conception est essentielle car elle permet de traduire les exigences en choix techniques et organisationnels concrets. Cette phase apparait avant le développement opérationnel pour s'assurer que l'architecture soit conçue de manière sécurisée. Cela va favoriser l'anticipation des failles en intégrant la sécurité « by design » plutôt que de la corriger après coût.

Il convient également de se poser des questions clés filtrantes proposées par le kit :

- L'architecture prévoit-elle des mécanismes de sécurité ? Cela inclut comme écrit l'authentification forte (MFA[10]), le cloisonnement réseau ou encore le chiffrement. Cela doit être prévu dans le design technique et validé par le RSSI.
- Les flux de données sont-ils identifiés et protégés ? Il faut ainsi réaliser une cartographie des flux pour visualiser tous les transits. L'objectif est de respecter la confidentialité, l'intégrité et la disponibilité des données.
- Des prestataires interviennent-ils ? Il est indispensable d'identifier les acteurs externes et de vérifier les clauses de conformité contractuelles en termes de sécurité. Cela évite ainsi les dérives.

[10] *Multi-factor authentification*

- Et enfin, les processus de gestion des incidents sont-ils documentés ? Cela signifie de prévoir comment seront gérées les violations de données ou tout incident de sécurité. Cela permet d'éviter une réponse improvisée en pleine phase d'exploitation.

Le kit poursuit cette phase en une série d'actions obligatoires :

- Une analyse d'impact RGPD si le projet manipule des données sensibles pour présente un risque élevé.
- Les clauses contractuelles de sécurité doivent être validées et signées avec les prestataires pour assurer les engagements de conformité.
- L'architecture doit être validée par el RSSI qui constitue ainsi un droit bloquant empêchant le projet d'avancer sans validation.

La conception organisée permet de lancer les projets après un cadrage technique sécurisé. Avec cette étape le chef de projet et le RSSI ont un cadre clair pour assurer la sécurité. Elle traduit les principes en architecture validée et contractualisée. Si l'architecture est solide, le projet peut avancer sereinement sans craindre des risques ou des négligences aux prochaines étapes.

1.3. Développement

Figure 20 : Kit des exigences de sécurité/RGPD - Développement (personnel)

La phase de développement marque le moment où, après la conception théorique, celui-ci est implémenté en solutions concrètes. C'est lors que cette étape que se joue la qualité du code ou les gestions des droits ainsi que la préparation des outils du supervision. Lorsque la sécurité n'est pas intégrée dès le développement, les failles perdureront jusqu'à la livraison du produit et seront bien plus difficiles et couteuses à corriger.

Selon ma proposition de kit les dimensions essentielles sont fondées sur trois aspects :

- La gestion des habilitations documentées. Selon le principe du moindre privilège, les accès doivent être répartis uniquement selon les rôles et leur nécessité. Cela évite les risques liés aux multiples portes d'entrées. Il faut ainsi documenter ces accès : qui accède à quoi, pourquoi et quel est son niveau d'autorisation.
- La revue de qualité du code. Le code produit pour le projet, donc l'ensemble des instructions informatiques, doit respecter les bonnes pratiques de sécurité. Cela se traduit par l'interdiction de stockage en clair[11] des mots de passe ou des données sensibles, la protection contre les attaques par injections (SQL)[12], la journalisation sécurisée des événements et le respect des normes de développement sécurisé (ANSSI).
- La préparation des outils de supervision. Avant même de mettre le projet en production, il faut anticiper les dispositifs de monitoring et de traçabilité afin de garantir que le système est observable et que les incidents pourront être détectés rapidement.

Pour cela la check-list de cette étape traduit ces exigences en une série d'actions obligatoires :

- Vérifier que les habilitations sont définies, documentées et validées
- Etablir une revue du code sécurisé
- Configurer les outils de supervision pour qu'ils soient opérationnels le plus rapidement possible.

Cette étape trouve son importance par le manque de documentation de suivi et permet ainsi d'obtenir des informations claires des évènements et des corrections de sécurité. Elle oblige également à intégrer la sécurité le plus vite possible.

La boucle corrective prévue dans le kit prend ici tout son sens : elle évite que des vulnérabilités se retrouvent en production. Si une faille est détectée, elle retourne en développement.

[11] *Il s'agit de tout fichier auquel il est possible d'accéder sans étape de protection particulière*

[12] *Type de vulnérabilité dans lequel un pirate utilise un morceau de code pour manipuler une base de données et accéder à des informations potentiellement importantes.*

1.4. Recette

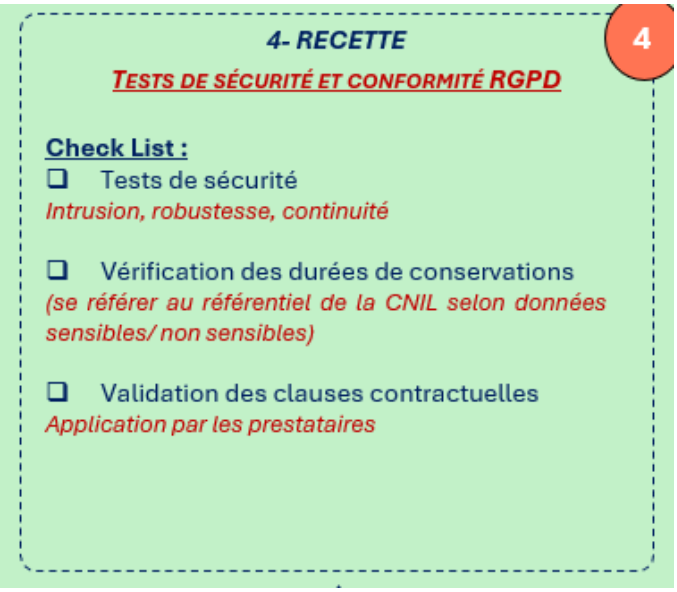

Figure 21 : Kit des exigences de sécurité/RGPD - Recette (personnel)

La phase de recette est la phase de vérification concrète des exigences de cybersécurité et RGPD définies lors des premières étapes.

C'est un point de contrôle bloquant, c'est-à-dire que si les exigences minimales ne sont pas respectées, le projet ne passera pas en production. Au cœur d'une collectivité cette étape est cruciale car les projets traitent très fréquemment des données sensibles, les failles mises en production peuvent avoir des impacts immédiats sur les citoyens et cela conditionne la confiance des usagers pour le service public.

Les questions essentielles s'articulent autour de vérifications :

- Les tests de sécurités ont-ils été réalisés ? Cela concerne les tests d'intrusion, les accès, les vérifications des failles connues…
- Les exigences RGPD sont-elles respectées ? Il convient de vérifier les durées de conservation, les destinataires… et bien évidemment vérifier qu'une analyse d'impact RGPD a été réalisée si données sensibles.
- Les habilitations et droits d'accès sont-ils conformes ? Il faut ainsi vérifier la matrice des habilitations.
- Les outils de supervision sont-ils opérationnels ? Cela signifie avoir une journalisation sécurisée, prévoir les alertes de sécurité fonctionnelles et avoir établi des procédures de gestion des incidents testées.

La check-list prévoit les actions à mener qui reprenne les questions évoquées :

- Le plan de tests sécurité
- Le check RGPD
- La validation des habilitations et des accès.
- Et pour finir la bonne application des clauses par les prestataires.

Les entretiens ont révélé des projets mis en production malgré des zones floues ou des validations incomplètes. La recette vient ainsi combler ces faiblesses. Elle oblige à formaliser les validations et permet d'offrir une traçabilité en cas d'accidents ultérieurs. Cette étape constitue le dernier verrou avant la mise en production afin de vérifier que tout est sûr et conforme. C'est également à la suite de cette étape que la boucle corrective intervient. Sans validation, chaque faille doit être retournée en développement pour garantir la sécurité du projet.

1.5. Mise en production

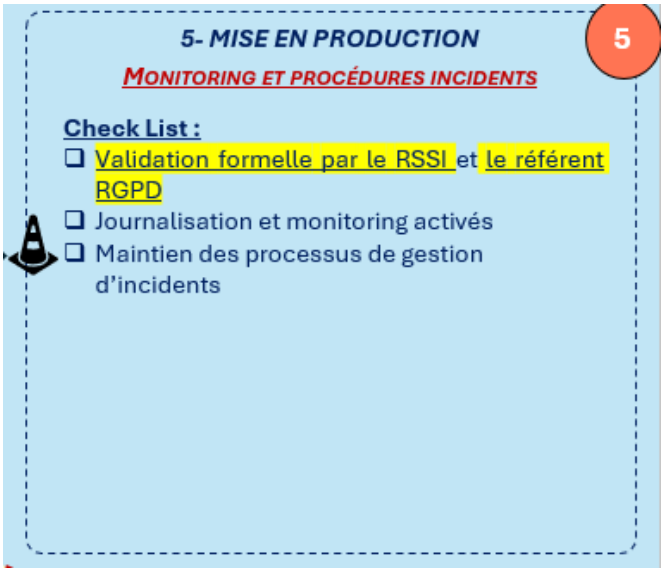

Figure 22 : Kit des exigences de sécurité/RGPD - Mise en production (personnel)

La mise en production est le moment bascule ou le projet n'est plus un projet mais devient accessible aux utilisateurs réels. Cette étape est critique car la moindre faille laissée peut compromettre la sécurité des données et des services.

Lors de cette étape nous allons vérifier plusieurs points. Dans un premier temps si les validations finales ont été obtenues. Le RSSI et el référent RGPD doivent avoir donné un Go explicite. Si une anomalie persiste, la mise en service doit être suspendue. Il faut également voir si les dispositifs de sécurité sont activés. La gestion des incidents doit être opérationnelle avec une procédure documentée et une équipe formée prête à intervenir. Cela passe également par la conformité des prestataires évoqués dans l'étape de recette.

La check list se constitue donc du check opérationnel final :

- Le Go des référents sécurité
- Les monitorings et les supervisions efficaces
- La procédure de gestion des incidents activée

La mise en production doit ainsi être formalisée comme un verrou final. Il faut s'assurer que rien n'est mis en place sans supervision et procédures actées. C'est un point de non-retour qui expose la collectivité aux menaces. C'est pourquoi cette étape doit être bloquante (illustré par un panneau de signalisation sur le document).

1.6. Exploitation/suivi

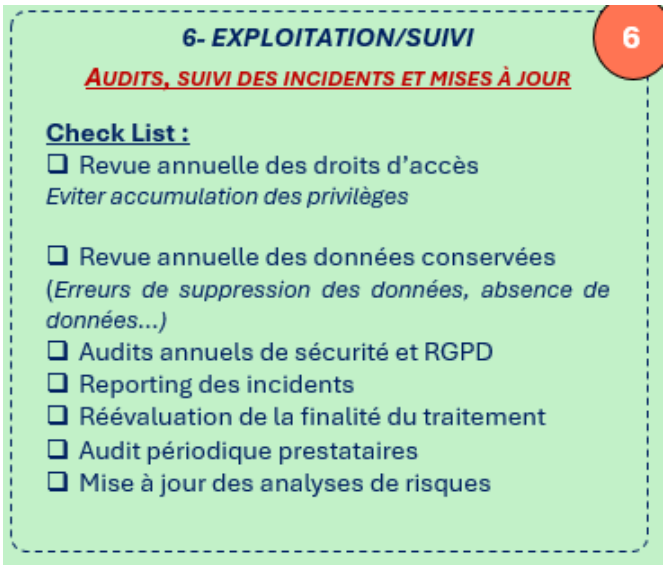

Figure 23 : Kit des exigences de sécurité/RGPD - Exploitation/Suivi (personnel)

Une fois que le projet est mis en production, la sécurité ne s'arrête pas. C'est un processus continu qui doit être assuré tout au long du cycle de vie.

La phase d'exploitation et de suivi vise donc à surveiller le système en fonctionnement, détecter et gérer les incidents, adapter les dispositifs selon les nouvelles menaces et réglementations et effectuer des audits réguliers pour garantir la conformité.

Il convient alors de réévaluer les risques régulièrement et mettre à jour la matrice des risques et bien sûr intégrer les retours d'incidents et les évolutions réglementaires.
Des audits doivent être réalisés sur la sécurité et la conformité. La supervision doit également être efficace en s'assurant des délais de résolution des alertes. Et pour finir la documentation doit absolument être mise à jour pour permettre un suivi fiable et actualisé.
La check list s'articule donc autour de plusieurs axes :

- Des audits annuels de sécurité et RGPD
- Du reporting régulier et de la prise en compte des incidents
- De la mise à jour de la matrice de risques
- Du suivi des prestataires

Cette phase vient répondre aux limites d'absence de retours et de manque de communication et procédures claires. Le but est d'instaurer un cycle permanent d'amélioration continue afin d'éviter les dérives et assurer la conformité face aux nouvelles réglementations.
L'exploitation et le suivi garantissent la pérennité de la cybersécurité et de la conformité RGPD. C'est une démarche dynamique qui nécessite des audits, des mises à jour régulière et une bonne gestion des incidents. Sans une démarche continue, un projet robuste au départ, peut devenir vulnérable au fil du temps.

2. Processus du Security by design

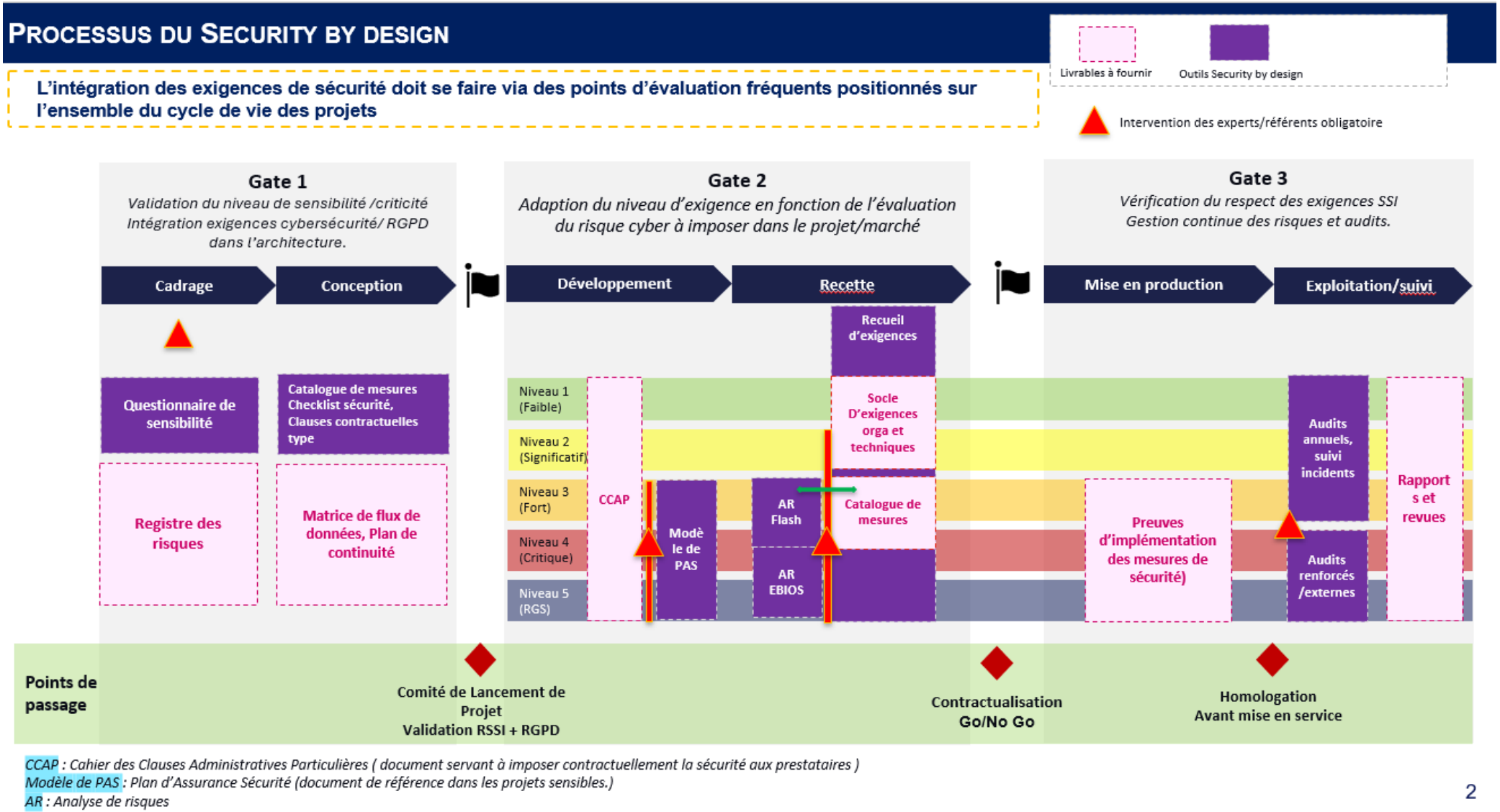

Figure 24 : Processus du Security by design (personnel)

Cette slide présentée illustre le processus de gestion de la cybersécurité intégré au cycle de vie des projets numériques. Ce schéma permet de matérialiser les moments clés ou la sécurité et la conformité RGPD doivent essentiellement être pris en compte. Celui-ci livre également les points de passage obligatoires ainsi que les livrables attendus.

L'intégration des exigences se structure autour de trois grandes étapes qui balisent la vie du projet. Ces trois grandes étapes reprennent chaque étape vue précédemment dans le kit.

- Gate 1 : Cadrage et conception = validation de la criticité du projet et homologation des premières exigences de sécurité
- Gate 2 : Développement et recette = adaptation du niveau des exigences selon les risques et mise en place des mesures adaptées
- Gate 3 : Mise en production et exploitation/suivi = vérification finale du projet, homologation et gestion continue des risques.

Toutes ces étapes sont pensées afin que la sécurité soit constamment prise en compte en l'intégrant dès le cadrage et en ajustant sa mise en place tout au long du projet.

Chaque phase nécessite des documents ou des preuves pour assurer la conformité. Cela peut paraitre redondant mais est essentiel pour formaliser et tracer la démarche du projet.

Le modèle intègre plusieurs niveaux de criticité qui permet d'adapter le niveau de sécurité aux enjeux du projet. En effet, un projet peu sensible ne nécessite pas les mêmes moyens qu'un projet très critique.

2.1. Gate 1

Ce premier Gate correspond donc aux phases 1 et 2 du kit : le cadrage et la conception. Lors du cadrage il est demandé de remplir le questionnaire de sensibilité et donc à partir de cela réaliser le registre des risques qui va permettre d'évaluer la criticité du projet. En enfin il va qualifier le projet en associant les données sensibles ainsi que le danger en cas de faille pour la collectivité.

Par la suite, lors de la conception, des outils comme le catalogue de mesures (document de référence qui regroupe l'ensemble des mesures organisationnelles techniques et juridiques nécessaires pour la conformité), la check list de sécurité (outils opérationnel simple qui permet

de vérifier que les principales exigences sont prises en compte dès la conception) et les clauses contractuelles types (modèles prérédigés qui sont insérés dans les contrats ou marchés publics qui vise à imposer la sécurité et le RGPD aux prestataires) vont permettre d'intégrer les premières exigences de sécurité et de RGPD dans l'architecture.

Les livrables attendus tel qu'une matrice des flux de données et un plan de continuité garantissent que les flux et les différentes dépendances soient cartographiés et protégés. Cela reflète les questions essentielles du kit sur les données personnelles, la criticité du projet et ses mécanismes de sécurité prévus.

Un point de passage est obligatoire à l'issu de la conception : le comité de lancement qui impose la validation par le RSSI et le DPO[13] avant de continuer le projet.

2.2. Gate 2

Le Gate 2 correspond aux phases 3 et 4 du kit : Développement et Recette

Lors du développement nous retrouvons les pratiques de sécurité dans le code : le modèle de PAS et la clause CCAP. Le modèle de PAS est le document de référence pour les projets sensibles qui décrit les mesures de sécurité mises en œuvre par le projet. La clause CCAP est quant à elle le document contractuel intégré dans les marchés publics et qui impose les obligations de sécurité juridiques des prestataires. La contractualisation se fait aux deux phases de conception et développement mais reste un prérequis au développement. C'est pourquoi cette étape est positionnée au tout début de la phase de développement.

Du côté recette on va vérifier la conformité SSI et RGPD avec le recueil des exigences, les analyses de risques ainsi que les socles d'exigences organisationnelles et techniques. L'analyse de risque Flash est une méthode simplifiée et rapide qui vise à analyser les risques. Elle est utilisée en début ou au cours du projet pour obtenir une vision claire et opérationnelle des principaux risques. L'analyse EBIOS pour les projets à fort risques est une méthode d'analyse complète et normalisée recommandée par l'ANSSI. Elle permet d'identifier les risques, définir les objectifs de sécurité et concevoir un plan d'action détaillé. On établit ainsi un catalogue des mesures qui est adapté selon les risques identifiés (revue de codes, habilitations, tests de sécurité, vérification des durées de conservation…).

[13] *Délégué à la protection des données*

Le point de passage est la contractualisation et donc le Go/ No Go, qui permet ainsi de décider si le projet peut passer en production.

2.3. Gate 3

Ce dernier Gate correspond aux phases 5 et 6 du kit : Mise en production et Exploitation/Suivi

La mise en production requiert des preuves d'implémentation telles que la journalisation, des monitoring opérationnels et des procédures officielles d'incident.

L'exploitation et le suivi nécessite des audits réguliers internes et externes mais également sur des rapports de suivi qui permettent de réévaluer et de suivre en continu la sécurité et la conformité RGPD.

Cela suit le kit à propos de la validation finale par le RSSI et le DPO ainsi que la gestion des incidents, les audits périodiques et la mise à jour des analyses de risques.

Le point de passage si situe à la fin de la phase de mise en production et consiste en l'homologation et donc la validation finale avant la mise en service.

2.4. Intervention des experts

Les triangles rouges signalent les étapes ou l'intervention des experts et des référents est obligatoire. Ils se situent dans la phase de cadrage pour valider la criticité ; en phase de conception/développement pour contrôler les clauses et les modèles de sécurité. Ils se trouvent également dans la phase de recette pour s'assurer de la bonne conformité technique et réglementaire et pour finir en phase d'exploitation pour garantir la pérennité des mesures.

Cela répond aux observations menées sur le terrain, les chefs de projets ne peuvent pas tout maitriser et doivent être accompagnés à des moments clés et soutenus par des spécialistes.

Comme appuyé dans le kit, la sécurité n'est pas figée. En effet les audits et retours d'expérience sont essentiels car permettent de réévaluer régulièrement les risques et d'ajuster les dispositifs. C'est un cycle vivant continu nécessaire face à l'évolution des menaces et des obligations.

3. Conclusion

La création de ce kit constitue ma réponse structurée aux difficultés que j'ai pu identifier lors de mon étude de terrain. Elaborée comme une boite à outils, il vise à accompagner, tel un guide simplifié et macro, les chefs de projets tout au long du cycle de vie des projets numériques en prenant en compte l'intégration progressive des exigences de sécurité et conformité réglementaire. Ce dispositif a ainsi pour but de :

- Clarifier les étapes clés par des phases concrètes, des outils assortis et les livrables attendus.
- Sécuriser les points de passages par des validation obligatoires avec l'intervention des experts aux moments critiques.
- Rendre les chefs de projet plus autonomes grâce à des supports simples et lisibles.

Le kit a donc été conçu pour répondre directement aux constats issus des entretiens tels que le manque de lisibilité, l'absence de procédure formalisée et structurée et la dépendance aux experts.

La réussite de ce kit dépend tout de même de deux conditions : L'appropriation du kit par les acteurs est essentielle. Celui-ci doit être diffusé et utilisé systématiquement pour que cela devienne un réflexe et un outil commun. Et enfin ce kit doit être mis à jour continuellement face aux évolutions fréquentes.

3.1. Les limites et perspectives du kit

Malgré l'avancée de ce kit en matière de structuration des exigences, celui-ci présente certaines limites à souligner pour en évaluer sa portée réelle.

Ce kit est un outil générique qui nécessite tout de même une adaptation au cas par cas. En effet ce kit est développé comme une base commune applicable à tous les projets numériques pour l'uniformité et la cohérence. Cependant il ne prend pas en compte les spécificités de chaque projet. Il est donc essentiel de la part des chefs de projet d'adapter et de contextualiser le kit en fonction de chaque projet et de sa sensibilité.

La région Île-de-France, comme de nombreuses collectivités, s'appuie particulièrement sur des prestataires. Le kit intègre cet aspect en prévoyant des clauses contractuelles types et des points de validation. Cependant cette dépendance peut créer des failles et des fragilités. Le respect de certaines exigences repose donc largement sur des acteurs extérieurs. L'objectif d'amélioration du Conseil Régional à long terme serait de réduire cette dépendance aux prestataires en renforçant les compétences en interne.

Ce kit élaboré s'inscrit dans une logique de simplification. Cependant les projets numériques sont soumis à bien d'autres exigences (accessibilité, archivage, Open data…). Le document présenté ne traite que des exigences de cybersécurité et de conformité RGPD et ne constitue pas un document unique consolidant l'ensemble des exigences des différentes verticales. L'enjeu serait donc d'évoluer vers un outil transversal et intégré permettant de disposer d'une vision globale de l'ensemble des exigences et des obligations applicables.

Comme tout référentiel ce kit est soumis au risque d'obsolescence. Les normes et menaces évoluant régulièrement, son usage efficace repose sur la mise à jour en continue afin que les exigences restent pertinentes et conformes au contexte.

4. Recommandations

A l'issue de mon étude de terrain et de mon année d'alternance, plusieurs idées de recommandations ont émergé pour permettre de renforcer la prise en compte de la cybersécurité dans les projets numériques de la Région Île de France. Ces recommandations ont pour objectif d'aider le conseil régional à corriger les manques identifiés, à simplifier la gouvernance et ainsi répondre à ma problématique.

4.1. Mettre en place un outil de suivi centralisé des projets

De nombreuses fois la question d'outil de suivi a été évoqué lors de diverses réunions. Aucune solution n'a été adoptée par tout le PTNum. Le suivi des projets et notamment des exigences et des étapes se fait de manière dispersée (fichiers, relances informelles, multiples outils…)

Je recommande donc de déployer un outil collaboratif simple tel que Microsoft List pour centraliser les informations clés de chaque projet. Dans le cadre de mes missions, j'ai eu l'occasion d'expérimenter l'outil Microsoft List pour le suivi et la gestion des étapes clés. Cet usage est très peu employé au sein de la Région car l'outil est peu connu et se heurte à une forte résistance au changement quand il s'agit de changer les habitudes des fichiers Excel et des échanges par mails. Pourtant son apport est très efficace. Il offre une vision claire et actualisée de l'avancée de chaque projet et permet de situer chaque validation. Il permet de regrouper les projets en un portefeuille centralisé accessible à tous les acteurs concernés. Cet usage constitue une piste intéressante dans la traçabilité et la gestion des projets numériques.
Dans la suite du Kit, cet outil permettrait le suivi des phases et Gate de manière très lisible et visuelle.

Les exemples ci-dessous sont des listes réalisées lors de projets que j'ai pu suivre aux cours de l'année. Certaines informations ont été masquées afin de garantir la confidentialité du projet.

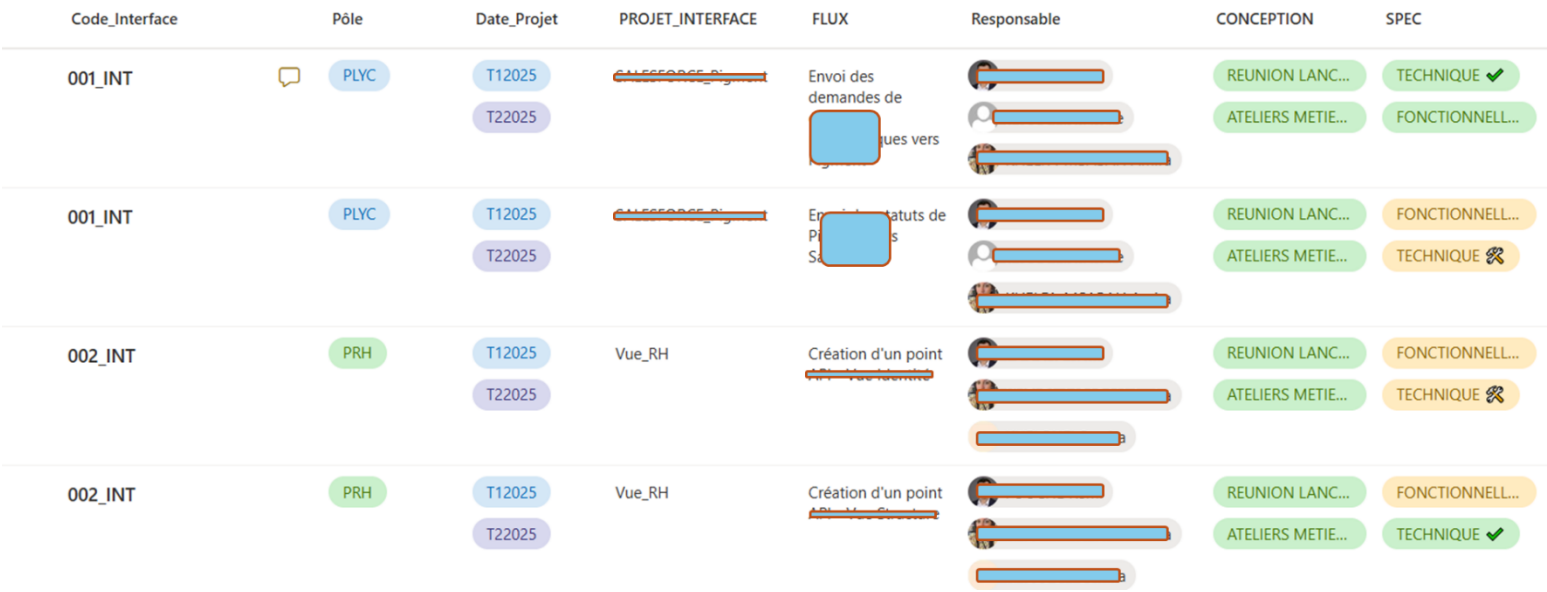

Figure 25 : Exemple d'utilisation de Microsoft List (personnel)

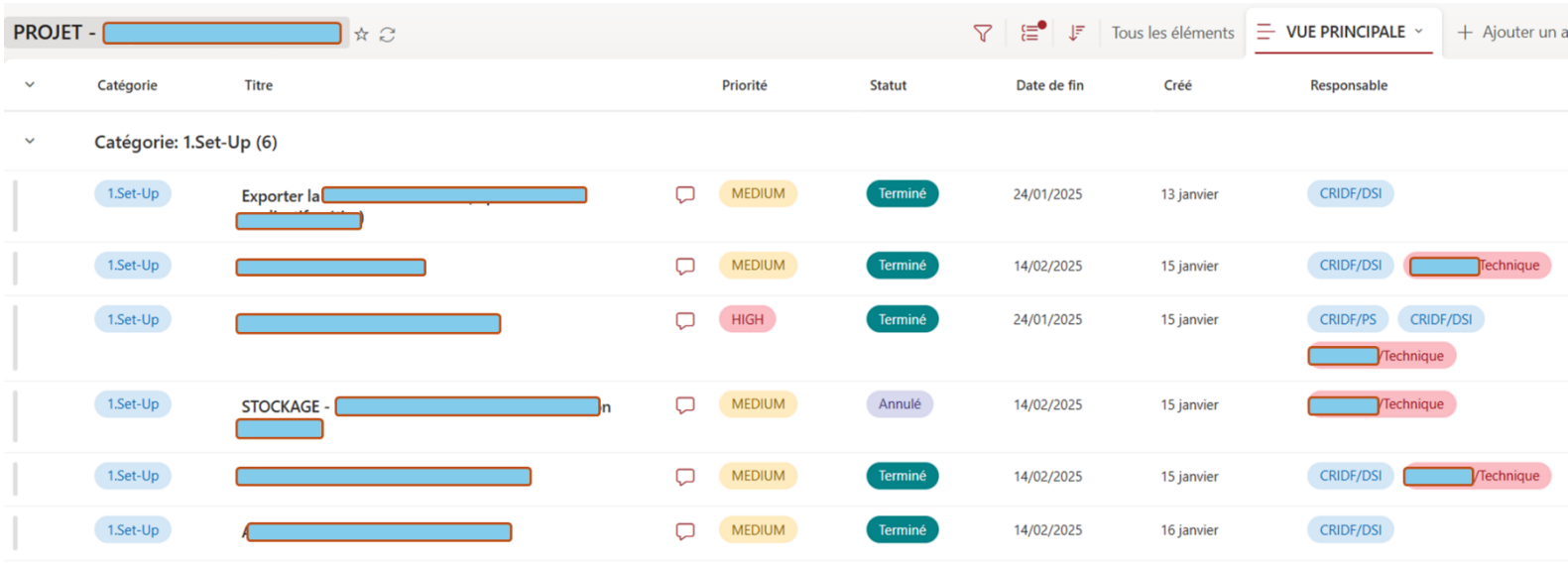

Figure 26 : Exemple d'utilisation de Microsoft List (personnel)

Ces exemples illustrent l'usage de Microsoft List pour le suivi des projets.
Le premier exemple correspond au suivi des projets d'interfaces. Chaque ligne correspond à une interface à mettre en place accompagné d'un suivi détaillé tel que les codes du projet, les flux, les dates, les pôles concernés ou encore l'état d'avancement des étapes. Il permet ainsi une visualisation synthétique et intuitive de l'avancement. Cette centralisation évite la dispersion des informations et est un outil collaboratif qui permet de voir l'état d'avancement des projets sans multiplier les échanges de mails.

Le second exemple présente une configuration utilisée pour le suivi opérationnel d'un projet. Chaque tâche est organisée en Set-Up avec une visibilité sur la priorité, le statut, les dates et les responsables. Ce format permet de hiérarchiser les actions et suivre les échéances pour avoir une vision de l'avancement global.

En définitive, Microsoft List s'avère être un outil particulièrement simple d'utilisation. La prise en main, y compris pour les utilisateurs peu familiers avec les solutions numériques, est très accessible. Son interface à la fois intuitive et visuelle permet une appropriation rapide et limite les freins liés à la technicité.
Cet outil constitue donc un véritable atout à long terme car il centralise les informations, améliore la traçabilité et renforce la transparence entre les acteurs.

4.2. Développer une sensibilisation continue et adaptée

Les formations ponctuelles sont largement insuffisantes pour une organisation aussi large et complexe que la Région Île-de-France. La sensibilisation constitue un pilier fondamental de toute stratégie de cybersécurité. Les entretiens menés ont montré un apprentissage « sur le tas » et la vision d'une cybersécurité parfois abstraite. Cela limite la capacité à anticiper les risques et intégrer les exigences de manière proactive. Pour pallier cette difficulté il faut pouvoir mettre en place une sensibilisation continue et adaptée qui se distingue de simples formations ponctuelles.

Cela se traduit par des rappels réguliers et concrets. Dans un premier temps la diffusion périodique de courtes communications ciblées tels que des « quotidiennes », dans le style d'une News Later, des réglementations et des nouveautés pourrait être bénéfique pour faire une piqure de rappel aux acteurs des projets. L'objectif serait d'ancrer des réflexes dans la durée en évitant l'effet « one shot » et à court terme d'une formation unique. Les formations viseraient à traduire les termes techniques, expliquer la cybersécurité et répondre aux question et incompréhension récurrentes.

Il serait également stimulant d'organiser des exercices pratiques et immersifs tels que des simulations d'attaques pour évaluer le comportement des agents face à des scénarios réalistes. Ces mises en situation sont encore trop peu pratiquées alors qu'elles permettent de mesurer le niveau de vigilance et de corriger les mauvaises pratiques ou allant directement aux sources du problème. Lors d'un recueil des besoins auprès d'un expert, celui-ci a expliqué que les simulations sont un moyen extrêmement efficace pour faire réaliser aux agents la facilité des attaques et les présences constantes des menaces.

Certaines sensibilisations et formations doivent être différenciées selon les publics. En effet il est stratégique d'adapter les communications en fonction des profils et des responsabilités. Par exemple les chefs de projet doivent être davantage sensibilisés sur les procédures, les agents métier sur la manipulation quotidienne des données et les prestataires sur l'intégration des clauses de sécurité. Cette approche vient compléter la sensibilisation générique peu efficace seule.

Et enfin une proposition d'accompagnement pourrait résider dans les points de contact entre les chefs de projets avec les référents et les experts. Les chefs de projet ne savent pas toujours vers qui se tourner pour poser des questions précises et reçoivent parfois peu ou pas de retours de la

part du RSSI et des experts qui sont finalement surchargés. Il pourrait être judicieux de mettre en place un canal dédié tel qu'un Canal Teams pour centraliser les questions, les bonnes pratiques ou les alertes liées à la sécurité. Cela permettrait de créer une culture partagée et de réduire l'isolement des acteurs.

4.3. Une meilleure gestion des habilitations et accès

La gestion des habilitations correspond aux règles et procédures qui permettent de définir qui a accès à quoi, quand et pourquoi. Une gestion bien gérée permet de limiter les risques d'intrusion ou les fuites de données. Cependant une gestion trop faible peut devenir une faille de sécurité majeure. La Région présente une forte accumulation d'habilitations non-mises à jour, cela créant des risques de droits excessifs et une mauvaise segmentation. En effet, le volume d'habilitation est très élevé du fait de la grande diversité de pôles et de projets. De plus le RSSI et son adjoint étant débordés et très opérationnels, ils ne peuvent assurer un suivi de chaque habilitation. Plusieurs mesures seraient judicieuses d'être mises en place

Dans un premier temps établir le principe du moindre privilège attribuerait uniquement les droits strictement nécessaires à l'exécution des missions. L'objectif est de limiter l'accès aux bases de données par des agents non concernés qui pourraient potentiellement causer des fuites de données. Cela s'accompagne d'une séparation des rôles notamment sur certaines taches critiques qui doivent être séparées pour éviter les abus. Par exemple, la validation d'une commande et son paiement doivent être effectuées par des personnes différentes pour renforcer le contrôle. Et enfin chaque accès à une base de données doit être nominatif afin d'assurer la traçabilité et la responsabilisation. Cela permet de garantir les pistes d'audit en cas d'incident.

Pour le suivi des habilitations un processus clair devrait être mis en place sans possibilité de dérogation.
Dans le cadre de l'attribution initiale, lors de l'arrivée d'un agent ou d'un prestataire, le processus doit être déclenché. Ses habilitations doivent être validées par le responsable hiérarchique et contrôlées par le référent sécurité. Toute demande devrait être documentée pour justifier le besoin d'accès.
Les habilitations sont amenées à évoluer en fonction des missions (changement de postes, nouveaux projets…). Une revue régulière des droits devrait être réalisée pour s'assurer de la

pertinence des accès. De plus, il faut absolument éviter les « comptes dormants » qui sont une porte d'entrée pour les attaquants.
Lors du départ d'un agent ou la fin d'un contrat, un processus de révocation des droits doit être activé et les accès coupés le jour même du départ et non plusieurs semaines après comme observé.
Une matrice des habilitations avec un tableau de référence indiquant les rôles et droits associés éviterait les demandes excessives ou incohérentes.

4.4. Renforcer la gouvernance et déléguer les responsabilités

L'un des constats observés lors de mon étude de terrain est la mobilisation trop importante du RSSI sur l'opérationnel au détriment de la vision stratégique malgré une délégation à un RSSI adjoint déployé sur les missions lycées.
Je recommanderais ainsi de déléguer une partie des tâches opérationnelles telles que les revues de code, les validations de checklists à des référents de cybersécurité au sein de chaque pôle ou bien d'agrandir l'équipe de sécurité afin de décharger le RSSI du surplus de taches. L'objectif serait de maintenir le RSSI sur les points stratégiques et bloquants et sur la sensibilisation de la cybersécurité. Son rôle se restreindrait aux validations finales, aux arbitrages et aux communications de sécurité. L'agrandissement peut se traduire par un adjoint RSSI supplémentaire ou une cellule de cybersécurité pour capitaliser sur les expertises en internes et fluidifier les échanges.

Conclusion Générale

Comme évoqué tout au long de ce mémoire la transformation numérique des collectivités territoriales représente une opportunité majeure pour la modernisation de l'action publique mais également pour l'organisation de toute structure.

Toutefois cette transformation s'accompagne d'une complexité accrue liée à la multiplication des projets numériques, à l'accélération des exigences réglementaires et à l'exposition croissante des menaces cyber. C'est dans ce système que la cybersécurité c'est imposé comme un enjeu systémique, dépassant largement le champ technique pour devenir par la suite une composante majeure de la gouvernance.

Ce mémoire avait pour but de répondre à la problématique suivante : *Comment piloter efficacement les exigences de cybersécurité dans un contexte organisationnel marqué par le manque de clarté, la fragmentation ou l'absence de procédure structurée ?*

L'analyse menée tout au long de ce travail a permis de montrer que la cybersécurité, souvent perçue comme illisible pour les non-experts et donc trop technique, constitue en réalité une mosaïques d'exigences allant du cadre européen et national jusuqu'aux procédures opérationnelles quotidienne. Ce constat est accentué dans les collectivités publiques soumises à des contraintes supplémentaires.

L'architecture pyramidale, étudiée précédemment, illustre la manière dont les différents niveaux (frameworks, politiques, standars et pratiques) viennent s'articuler pour créer un disposotif global nécéssaire pour difficilement appréhendé par les chefs de projet.

Mon étude menée au sein du Conseil régional d'Île-de-France a démontré ces constats. En effet j'ai pu observer et mettre en évidence la fragmentation des responsabilités, le manque de compréhension des outils d'accompagnement et la difficulté à traduire les obligations nombreuses en actions concrètres.

La valeur ajoutée de mon mémoire résulte ainsi dans la mise en lumière de ces écarts entre prescritpion théorique et les réalités pratiques du terrain mais également dans l'identification de leviers pour remédier à ces écarts. Parmis ces mesures, la nécéssité de développer des outils méthodologiques plus adaptés aux chefs de projet : kit de pilotage, guides simplifiés, dispositifs de sensibilisation. Ces solutions font parties des facteurs clés pour renforcer la compréhension et la capcité des chefs de projet dans l'intégration de la cybersécurité dès la conception des projets numériques.

Limites du travail de recherche et ouverture

Néanmoins, le travail effectué présente certaines limites.
Dans un premier, mon étude ne repose que sur une seule organisation : le Conseil régional d'Île-de-France, une grande organisation publique. Cela ne permet pas une généralisation des résultats à toutes les organisations et à l'ensemble des collectivités. De plus mon étude s'est concentrée sur le contexte public. Cependant les dynamiques internes ainsi que les ressources sont souvent bien différentes de celles du secteur privé. Les constats émis dans mon étude de terrain doivent donc être lus à la lumière du contexte.

Ensuite le nombre de personnes interrogées dans le cadre de mes entretiens reste relativement restreint. Mes échanges se sont concentrés majoritairement sur des personnes occupant des rôles clés et bien que cela permet de dégager des constats pertinents, un panel plus large aurait permis de croiser d'avantages de points de vue pour appuyer ma réflexion.

Par ailleurs, ce mémoire a été réalisé dans le cadre d'une expérience limitée au sein de l'entreprise. En effet, la position d'alternant, bien qu'offrant une position d'observateur privilégié, a pu restreindre l'accès en informations stratégiques ou à des processus internes plus sensibles. De plus, la durée d'un an dans l'entreprise m'a permis d'acquérir une certaine vision opérationnelle mais ne m'a pas donnée accès à l'ensemble des dynamiques stratégiques en arrière-plan.

D'autre part les évolutions très rapides du cadre réglementaires et des menaces impose une vigilance constante. Cela rend toutes les analyses ainsi que les outils susceptibles d'être rapidement dépassés. Il faut savoir se renouveler et s'adapter en permanence ainsi qu'adapter les pratiques en fonction du contexte et de la maturité de l'organisation.

Ces limites invitent donc à reconsidérer ce mémoire comme une piste d'analyse et de recommandations pratiques. Celles-ci doivent êtres par la suite enrichis de travaux sur d'autres terrains et auprès d'un plus grand panel d'acteurs.
Cela ouvre la voie à de futures recherches notamment sur la sensibilisation par fausses mises en situation ou fausses attaques. De plus, il serait pertinent de s'appuyer sur le développement d'outils d'aide à la décision fondés sur l'intelligence artificielle ou sur les jumeaux numériques pour accompagner les futurs projets. Pour les collectivités territoriales, les conditions

indispensables résident dans le renforcement de la gouvernance cyber, la clarification des responsabilités et l'outillage des chefs de projets afin de garantir la continuité des services et de préserver la confiance des citoyens.

Bibliographie

[Abrahams et al., 2024] T. O. Abrahams, S. K. Ewuga, S. O. Dawodu, A. O. Adegbite, A. O. Hassan. *A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection*. Computer Science & IT Research Journal, vol. 5, no. 1, 2024, pp. 1–25.

[Alexander, 2024] A. Alexander, C. Asset Security and Asset Management: *Cybersecurity Case Study of a Large Medical Center.* General Medicine and Clinical Practice, 7(9), 2024, pp. 01–04.

[Aleroud et al, 2017] A. Aleroud, L. Zhou. *Phishing environments, techniques, and countermeasures: A survey.* Computers & Security, 68, 2017, pp. 160–196.

[AlGhamdi et al., 2020] S. AlGhamdi, K. T. Win, E. Vlahu-Gjorgievska. *Information security governance challenges and critical success factors: Systematic review.* Computers & Security, 99, 2020, pp. 102030.

[Animashaun et al., 2024] E. Animashaun, B. T. Familoni, N. C. Onyebuchi. *Strategic project management for digital transformations in public sector education systems.* International Journal of Management & Entrepreneurship Research, 6(6), 2024, pp. 1813–1823.

[Ardi et al., 2023] S. Ardi, K. Sandahl, M. Gustafsson. A Case Study of *Introducing Security Risk Assessment in Requirements Engineering in a Large Organization.* SN Computer Science, 4(5), 2023, pp. 488.

[Attrill-Smith et al., 2019] A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss. *The Oxford Handbook of Cyberpsychology*. Oxford : Oxford University Press, 2019. ISBN : 978-0-19-881274-6.

[Bada et al., 2015] M. Bada, A. M. Sasse, J. R. C. Nurse. *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* International Conference on Cyber Security for Sustainable Society (CSSS 2015), Oxford, UK, 2015. Global Cyber Security Capacity Centre, University of Oxford.

[Baumeister et al., 2007] R. F. Baumeister, K. D. Vohs, M. E. Tice. *The strength model of self-control.* Current Directions in Psychological Science, vol. 16, no. 6, 2007, pp. 351–355.

[Bertaud du Chazaud et al, 2020] J. Bertaud du Chazaud, J., É. Delisle. *Enjeux éthiques du numérique dans le secteur social : rôle et réflexions de la CNIL*: Vie sociale, n° 28(4), 2020, pp. 65–76.

[Birnbaum et al., 2005] R. Birnbaum, C. M. Christensen, M. E. Raynor. *The innovator's dilemma: When new technologies cause great firms to fail*. Academe, vol. 91, no. 1, 2005, p. 80.

[Boulesnane et al., 2020] S. Boulesnane, C. Varinard, L. Bouzidi. *RGPD et e-administration : besoins, pratiques et défis*. Documentation et bibliothèques, vol. 65, no. 4, 2020, pp. 102–120.

[Bourey et al., 2010] J.-P. Bourey, Y. Ducq, A. Cauvin, D. Crestani, et al. *Méthodologie d'ingénierie des systèmes d'entreprise centrée sur les modèles : application au pilotage de la performance durable.* Thèse de doctorat en sciences, présentée par Nawel Amokrane, Université Bordeaux 1, 2010.

[Brill et al., 2006] J. M. Brill, M. J. Bishop, A. E. Walker. *The competencies and characteristics required of an effective project manager: A web-based Delphi study*. Educational Technology Research and Development, vol. 54, no. 2, 2006, pp. 115–140.

[Canzittu, 2022] D. Canzittu. *A framework to think of school and career guidance in a VUCA world.* British Journal of Guidance & Counselling, 50(2), 2022, pp. 248–259.

[CFTL, 2011] CFTL/REQB. *Glossaire des termes utilisés en ingénierie des exigences*, version 1.3, Comité Français des Tests Logiciels, 16 août 2011, 16 p. Traduction française d'après IEEE 610.

[Chavanne, 2017] J.-S. Chavanne. *Le numérique à tous les étages : le rôle de l'Anssi:* I2D - Information, données & documents, Volume 54(2), 2017, pp. 37–38.

[Cheimonidis & Rantos, 2023] P. Cheimonidis, K. Rantos. *Dynamic risk assessment in cybersecurity: A systematic literature review*. Future Internet, vol. 15, no. 10, 2023, p. 324.

[Cicmil et al., 2006] S. Cicmil, T. Williams, J. Thomas, D. Hodgson. *Rethinking project management*: *Researching the actuality of projects*. International Journal of Project Management, vol. 24, no. 8, 2006, pp. 675–686.

[Clegg et al., 2018] S. Clegg, C. P. Killen, C. Biesenthal, S. Sankaran. Practices, projects and portfolios: Current research trends and new directions. International Journal of Project Management, vol. 36, no. 5, 2018, pp. 762–772.

[Craigen et al., 2014] D. Craigen, N. Diakun-Thibault, R. Purse. *Defining cybersecurity. Technology Innovation Management Review,* vol. 4, no. 10, 2014, pp. 13–21.

[Delorme, 2023] G. Delorme. *Aide à la gestion de l'impact des stratégies IT sur la maîtrise du risque réglementaire.* Thèse de doctorat (Informatique), Université Jean Moulin Lyon 3 – Université de Lyon, 28 mars 2023. NNT : 2023LYO30008.

[Doray, 1992] P. Doray. Claude Dubar, *La socialisation, construction des identités sociales et professionnelles*, Paris, Armand Colin, 1991, 278 p. Cahiers de recherche sociologique, nos 18–19, 1992, p. 308.

[Douville, 2020] T. Douville. *L'émergence des cyber-risques*. Archives de philosophie du droit, tome 62(1), 2020, pp. 289–298.

[Dupont, 2017] B. Dupont. *La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale*. In B. Dupont (dir.), La gouvernance du cyberespace : quel rôle pour l'État ? Paris : L'Harmattan, 2017, pp. 53–78. ISBN 978-2-343-10075-3.

[Ferguson-Walter et al., 2021] K. J. Ferguson-Walter, M. M. Major, C. K. Johnson, D. H. Muhleman. *Examining the efficacy of decoy-based and psychological cyber deception.* Proceedings of the 30th USENIX Security Symposium, 2021, pp. 1127–1139. USENIX Association.

[Forscey et al., 2022] D. Forscey, J. Bateman, N. Beecroft, B. Woods. *Systemic cyber risk: A primer.* Carnegie Endowment for International Peace & Aspen Institute, Washington D.C., 2022, 27 p.

[Furnell, 2008] S. Furnell. *End-user security culture: A lesson that will never be learnt?* Computer Fraud & Security, vol. 2008, no. 4, avril 2008, pp. 6–13.

[Garza et al., 2022] C. D. L. Garza, S. Charles, N. Oufi. *Prise en compte des facteurs organisationnels et humains en cybersécurité : aller au-delà de l'erreur humaine*. Congrès Lambda Mu 23 – Innovations et maîtrise des risques pour un avenir durable, Institut pour la Maîtrise des Risques, oct. 2022, Saclay, France. ffhal-03966636.

[Gollmann, 2011] D. Gollmann. *Computer Security* (3e édition). Wiley, Chichester, 2011. ISBN 978-0-470-74115-3.

[Hilary et al, 2024] G. Hilary, V. Serret. *Gouvernance et transformation numérique.* Finance Contrôle Stratégie, 27–1, 2024.

[Hoffmann et al., 2020] R. Hoffmann, J. Napiórkowski, T. Protasowicki, J. Stanik. *Risk-based approach in scope of cybersecurity threats and requirements*. Procedia Manufacturing, vol. 44, 2020, pp. 655–662.

[Karabacak et al., 2016] B. Karabacak, S. Ozkan Yildirim, N. Baykal. *A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness.* International Journal of Critical Infrastructure Protection, vol. 15, 2016, pp. 47–59.

[Kerzner, 2004] H. Kerzner. *Advanced Project Management: Best Practices on Implementation*. 2e édition. Hoboken, NJ : John Wiley & Sons, 2004.

[Kloetzer, 2015] H. Kloetzer. *La maîtrise d'ouvrage des projets informatiques. Chapitre 1 : Définition et lancement des projets informatiques*. Paris : Lavoisier, 2015, pp. 1-13.

[Kianpour & Raza, 2024] M. Kianpour, S. Raza. *More than malware: Unmasking the hidden risk of cybersecurity regulations*. International Cybersecurity Law Review, vol. 5, no. 1, 2024, pp. 169–212.

[Knockaert, 2019] M. Knockaert. *La sécurité dans le marché unique numérique européen : le Règlement 2019/881* (« Cybersecurity Act »). Dans Les obligations légales de cybersécurité et de notifications d'incidents. Bruxelles : Politeia, 2019, pp. 157–180.

[Kremer et al., 2019] S. Kremer, L. Mé, D. Rémy, V. Roca. *Cybersécurité : défis actuels et axes de recherche à l'Inria* (résumé du livre blanc). Inria, 2019.

[Larson et al, 2011] E. W. Larson, & C. F. Gray. *Project Management: The Managerial Process*. 5e édition. New York : McGraw-Hill Higher Education, 2011.

[m, 2021] J. Lepage. *Les impacts de la transition numérique sur les métiers de la fonction publique territoriale. Volet prospectif*. Paris : CNFPT, octobre 2021, 86 p.

[Lundgren et al, 2019] B. Lundgren, N. Möller. *Defining information security. Science and Engineering Ethics*, vol. 25, no. 2, 2019, pp. 419–441.

[Marchand, 2024] J. Marchand. *Cybersécurité et traitement des données personnelles par les collectivités territoriales*. Étude. JCP A – La Semaine Juridique Administrations et collectivités territoriales, n° 21, 27 mai 2024, 2148.

[Marhraoui, 2023] M. A. Marhraoui. *Digital Skills for Project Managers: A Systematic Literature Review*. Procedia Computer Science, 219, 2023, pp. 1591–1598.

[Masse et al., 2017] F. Masse, H. Abdo, J.-M. Flaus. V*ers une approche intégrant les exigences de cybersécurité à la maîtrise des risques d'accidents majeurs pour les ICPE.* 12e Congrès International Pluridisciplinaire en Qualité, Sûreté de fonctionnement et Développement durable (QUALITA 2017), Bourges, France, août 2017. HAL.

[Mattatia, 2019] F. Mattatia. *RGPD et droit des données personnelles*, 4e édition. Paris : Eyrolles, 29 août 2019. ISBN 978-2-212-67839-0.

[Maury, 2022] E. Maury. *La CNIL face aux enjeux de la construction d'une société numérique de confiance: Annales des Mines* - Réalités industrielles, Août 2022(3), 2022, pp. 75–78.

[Mohamad et al., 2024] M. Mohamad, J.-P. Steghöfer, E. Knauss, R. Scandariato. *Managing security evidence in safety-critical organizations.* arXiv preprint, arXiv:2404.17332 [cs.SE], 26 avril 2024.

[Müller et al., 2018] N. Drouin, S. Sankaran, R. Müller. *Balancing person-centric and team-centric leadership in projects*. White Paper, Project Management Institute (PMI), mai 2018.

[Nehari Talet, 2022] A. Nehari Talet. *The Effect of Digital Transformation on Information Systems Development*. International Journal of Computers, 7, 2022, pp. 138–156. ISSN: 2367-8895.

[Nobles, 2018] C. Nobles. *Botching Human Factors in Cybersecurity in Business Organizations*. HOLISTICA – Journal of Business and Public Administration, 9(3), 2018, pp. 71–88.

[Norman, 2017] K. L. Norman. *Cyberpsychology: An Introduction to Human-Computer Interaction.* Cambridge : Cambridge University Press, 2017. ISBN : 978-1107102540.

[Ochoa Pacheco et al., 2023] P. Ochoa Pacheco, D. Coello-Montecel, M. Tello, V. Lasio, A. Armijos. *How do project managers' competencies impact project success?* A systematic literature review. PLOS ONE, 18(12), 2023, pp. e0295417.

[O'Kane et al., 2018] P. O'Kane, S. Sezer, D. Carlin. Evolution of ransomware. IET Networks, vol. 7, no. 5, 2018, pp. 321–327.

[Panteli et al., 2025] N. Panteli, B. R. Nthubu, K. Mersinas. *Being responsible in cybersecurity: A multi-layered perspective*. Information Systems Frontiers, 2025.

[Parsons et al., 2014] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, C. Jerram. *Determining employee awareness using the Human Aspects of Information* Security Questionnaire (HAIS-Q). Computers & Security, vol. 42, 2014, pp. 165–176.

[Paul et al., 2021] S. Paul, N. Van Cauter, P. Varela, S. Leboeuf, M. Catroux. *Systématisation d'une démarche de sécurisation par conformité ajustée aux besoins et enjeux de sécurité – une revue critique*. Proceedings of the 28th C&ESAR, Rennes, 16–17 novembre 2021. CEUR Workshop Proceedings, 2021.
[Perinet et al, 2010] R. Perinet, T. N. Vu. Évaluer la fiabilité humaine : quelle(s) méthode(s) choisir ? Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda-Mu 17, La Rochelle, France, octobre 2010, pp. Comm 1B-1. ffineris-00973592.

[Pisa et al, 2013] B. J. Pisa, A. G. de Oliveira. *Gestão de projetos na administração pública: um instrumento para o planejamento e desenvolvimento.* Seminário Nacional de Planejamento e Desenvolvimento, 2013. Universidade Tecnológica Federal do Paraná (UTFPR).

[Ponsard et al., 2022] C. Ponsard, V. Ramon, M. Touzani. Méta-modèle des concepts et processus d'analyse des risques selon les normes de cybersécurité. 2022.

[Ramirez et al, 2016] R. Ramirez, N. Choucri. *Improving interdisciplinary communication with standardized cyber security terminology: A literature review*. IEEE Access, vol. 4, 2016, pp. 2216–2243.

[Rhee et al., 2009] H.-S. Rhee, C. Kim, Y. U. Ryu. *Self-efficacy in information security: Its influence on end users' information security practice behavior.* Computers & Security, vol. 28, no. 8, 2009, pp. 816–826.

[Saeed et al., 2023] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, D. A. Alabbad. *Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations*. Sensors, vol. 23, no. 15, 2023, p. 6666.

[Salahdine et al, 2019] F. Salahdine, N. Kaabouch. *Social engineering attacks: A survey*. Future Internet, vol. 11, no. 4, 2019, p. 89.

[Salvaggio et al, 2023] S. A. Salvaggio, N. González. *The European framework for cybersecurity: Strong assets, intricate history.* International Cybersecurity Law Review, vol. 4, no. 1, 2023, pp. 137–146.

[Santos-Neto et al, 2019] J. B. S. D. Santos-Neto, A. P. C. S. Costa. *Enterprise maturity models: A systematic literature review*. Enterprise Information Systems, vol. 13, no. 5, 2019, pp. 719–769.

[Sasse et al., 2001] M. A. Sasse, S. Brostoff, D. Weirich. *Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security*. BT Technology Journal, vol. 19, no. 3, 2001, pp. 122–131.

[Schatz et al., 2017] D. Schatz, R. Bashroush, J. Wall. *Towards a more representative definition of cyber security.* The Journal of Digital Forensics, Security and Law, 2017.

[Staili et al, 2024] S. E. Staili, N. Bencherif. Sécurité dans les réseaux sans fil (Wi-Fi). Mémoire de Master académique, Spécialité Systèmes des télécommunications, Université Abdelhamid Ibn Badis – Mostaganem, Faculté des Sciences et de la Technologie, Département de Génie Électrique, soutenu le 26 juin 2024.

[Strubel, 2023] V. Strubel. *L'ANSSI, le garant de la cybersécurité et de la cyberdéfense de la France.* La Jaune et la Rouge, no. 795, Cahier no. 2, juin 2023, pp. 4–6.
[SWEBOK, 2014] Bourque, P., R. E. Fairley (Eds.). *Guide to the Software Engineering Body of Knowledge (SWEBOK® Guide), Version 3.0*. IEEE Computer Society, 2014

[Szpitter et al., 2016] A. Szpitter, J. Sadkowska. *Using VUCA matrix for the assessment of project environment risk*. Zarządzanie i Finanse (Journal of Management and Finance), vol. 14, no. 2/1, 2016, pp. 401–413.

[Ventre, 2015] D. Ventre. *Les évolutions de la cybersécurité : contraintes, facteurs, variables….* Étude prospective et stratégique n° 1506388759, Ministère de la Défense – Direction générale des relations internationales et de la stratégie (DGRIS), juin 2015.

[Villamizar et al., 2018] H. Villamizar, M. Kalinowski, M. Viana, D. M. Fernandez. *A systematic mapping study on security in agile requirements engineering*. 2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), Prague, 2018, pp. 454–461.

[Walden, 2005] I. Walden. *Crime and Security in Cyberspace*. Cambridge Review of International Affairs, 18(1), 2005, pp. 51–68.

[Wanderley et al., 2014] F. Wanderley, N. Belloir, J.-M. Bruel, N. Hameurlain, J. Araújo. *Des buts à la modélisation système : une approche de modélisation des exigences centrée utilisateur.* 2014.

[Weinstein, 1980] N. D. Weinstein. *Unrealistic optimism about future life events*. Journal of Personality and Social Psychology, vol. 39, no. 5, 1er novembre 1980, pp. 806-820.

[Wiener, 2014] N. Wiener. *Cybernétique et société : l'usage humain des êtres humains*. Paris : Éditions du Seuil, coll. « Points / Sciences » (S216), 2014. ISBN 978-2-7578-4278-2.

[Woods et al., 2017] D. Woods, I. Agrafiotis, J. R. C. Nurse, S. Creese. *Mapping the coverage of security controls in cyber insurance proposal forms*. Journal of Internet Services and Applications, vol. 8, no. 1, 2017, p. 8.

Webographie

[Accenture, 2025] Accenture. *Only one in 10 organizations globally are ready to protect against AI-augmented cyber threats*. Accenture Newsroom, 2025. Disponible sur : https://newsroom.accenture.com/news/2025/only-one-in-10-organizations-globally-are-ready-to-protect-against-ai-augmented-cyber-threats

[ANSSI, 2024] CERT-FR (ANSSI). Rapport d'analyse de la menace informatique 2024. Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR), Agence nationale de la sécurité des systèmes d'information (ANSSI), Paris, janvier 2024. Disponible sur : https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-001/

[Bluefin, 2025] Bluefin. *IBM's 2025 Data Breach Report: Key findings and the year's biggest attacks*. Bluefin News, 2025. Disponible sur : https://www.bluefin.com/bluefin-news/ibms-2025-data-breach-report-key-findings-and-the-years-biggest-attacks/

[CGV-Expert, s.d.] CGV-Expert. LCEN (Loi pour la confiance dans l'économie numérique) : prestation, rédaction & conditions générales. CGV-Expert, sans date. Disponible sur : https://www.cgv-expert.fr/prestation-redaction-conditions-generales/lcen-loi-confiance-economie-numerique

[CNIL, s.d.] Commission Nationale de l'Informatique et des Libertés. Règlement européen protection des données. CNIL, sans date. Disponible sur : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

[Devillers, 2025] O. Devillers. *Accessibilité numérique : 96 % des sites communaux sont non conformes*. Localtis pour la Banque des Territoires, 2025. Disponible sur : https://www.banquedesterritoires.fr/accessibilite-numerique-96-des-sites-communaux-sont-non-conformes

[Indeed, 2024] Indeed. Les 10 compétences organisationnelles incontournables. Indeed France, mis à jour le 15 août 2024. Disponible sur : https://fr.indeed.com/conseils-carrieres/trouver-un-emploi/competences-organisationnelles-incontournables

[ITPro, 2025] ITPro. *Lack of visibility creates cascade of security risk, says Kiteworks*. ITPro, 2025. Disponible sur : https://www.itpro.com/business/business-strategy/lack-of-visibility-creates-cascade-of-security-risk-says-kiteworks

[Keepnet Labs, 2025] Keepnet Labs. *2025 Verizon Data Breach Investigations Report*. Keepnet Labs Blog, 2025. Disponible sur : https://keepnetlabs.com/blog/2025-verizon-data-breach-investigations-report

[Leto Legal, 2022] Leto Legal. Qu'est-ce que la CNIL ?. Leto Legal Guides, 30 novembre 2022. Disponible sur : https://www.leto.legal/guides/quest-ce-que-la-cnil

[Ministère de l'Économie, 2025a] Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique. Comment se prémunir contre l'hameçonnage ?. Gouvernement.fr, 2025. Disponible sur : https://www.economie.gouv.fr/particuliers/numerique-et-cybersecurite/comment-se-premunir-contre-lhameconnage#

[Ministère de l'Économie, 2025b] Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique. Cinq conseils pour se prémunir contre les rançongiciels : Assurer sa cybersécurité et la protection de ses données. Économie.gouv.fr, 2025. Disponible sur : https://www.economie.gouv.fr/entreprises/assurer-sa-cybersecurite-et-la-protection-de-ses-donnees/cinq-conseils-pour-se-premunir#

[NIS-2 Directive, s.d.] Cyber Risk GmbH. Articles – NIS 2 Directive: final text. NIS-2-Directive.com. Disponible sur : https://www.nis-2-directive.com/NIS_2_Directive_Articles.html

[Perrin, 2021] C. Perrin. *Archivage des marchés publics issus de la dématérialisation*. Question écrite n° 23503 – 15e législature, Sénat, publiée le 24 juin 2021, réponse du ministère de la Culture le 2 septembre 2021. Disponible sur : https://www.senat.fr/questions/base/2021/qSEQ210623503.html

[PwC, 2024] PwC. 2025 Global Digital Trust Insights. PwC Global, 2024. Disponible sur : https://www.pwc.com/gx/en/news-room/press-releases/2024/pwc-2025-global-digital-trust-insights.html

[Service-Industrie, s.d.] Service-Industrie. Quel est l'objectif de la loi LCEN ?. Service-Industrie, sans date. Disponible sur : https://www.service-industrie.fr/quel-est-lobjectif-de-la-loi-lcen.html#:~:text=L'objectif%20principal%20de%20la,dans%20le%20milieu%20du%20web marketing

[Visiativ, 2024] Visiativ. Baromètre : la cybersécurité des entreprises françaises, édition 2024. Visiativ Actualités, 2024. Disponible sur : https://www.visiativ.com/actualites/actualites/barometre-la-cybersecurite-des-entreprises-francaises-edition-2024/

[Wavestone, 2025] Wavestone. *2025 Cyber Benchmark: Measured progress, persistent challenges*. Wavestone Insight, 2025. Disponible sur : https://www.wavestone.com/en/insight/2025-cyber-benchmark-measured-progress-persistent-challenges/

[World Economic Forum, 2025] World Economic Forum en collaboration avec Accenture. *Global Cybersecurity Outlook 2025*. Publié le 13 janvier 2025. Disponible sur : https://www.weforum.org/publications/global-cybersecurity-outlook-2025/