cyber eco

GUIDE

Le programme Imperium

Outiller votre organisation à systématiser et accélérer l'identification de l'efficacité de vos contrôles de sécurité de l'information

Le programme Imperium

Ce guide a été créé pour vous aider à mettre en place le programme de modernisation de la gouvernance de sécurité de l'information, nommé Imperium, dans votre organisation. Ce programme vous permettra de systématiser et accélérer l'identification de l'efficacité des contrôles de sécurité de l'information dont votre organisation a besoin.

Il est utile pour accompagner tout professionnel, œuvrant en sécurité de l'information, dans une entreprise qui a une équipe interne ayant la capacité de coordonner la gestion d'un programme de sécurité[1]. Il s'adresse aux entreprises de tous les secteurs d'activités allant du bancaire au commerce de détails en passant par l'énergie, la santé, les technologies de l'information, les services publics et plus encore.

Le guide est divisé en trois grandes sections :

1. Qu'est-ce que le programme Imperium et pourquoi devriez-vous le mettre en place dans votre organisation ?
2. Quels sont les facteurs de succès préalable à la mise en place du programme Imperium dans votre organisation ?
3. Quelles sont les étapes de mise en place du programme Imperium dans votre organisation ?

Pour davantage de questions ou besoin d'accompagnement contacter CyberEco.

Bonne lecture !

[1] Une version adaptée du présent guide sera créée afin d'accompagner les entreprises de plus petites tailles n'ayant pas d'équipe interne pouvant coordonner la gestion d'un programme de sécurité de l'information.

Table des matières

Qu'est-ce que le programme Imperium et pourquoi devriez-vous le mettre en place dans votre organisation ? 4

Quels sont les facteurs de succès préalables à la mise en place du programme Imperium ? 6

1. Création d'une équipe centrale et identification du promoteur exécutif 6
2. La préparation du terrain 8

Support exécutif 8

Création d'un plan de déploiement 9

Mobilisation des parties prenantes 10

Quelles sont les étapes de mise en place du programme Imperium ? 11

1. S'approprier la méthodologie 12

Rôles et responsabilités 12

Cadre de contrôles 18

Tableaux de bord de suivi 26

2. Rédiger le plan d'évaluation 32

Outil de collecte 33

Déclencheurs d'évaluation 34

Objectifs d'évaluation (exigences) et portée 36

Niveau de confiance attendu 38

3. Réaliser l'évaluation des contrôles 39

Évaluation par les propriétaires de contrôles 41

Revue de cohérence des résultats 42

4. Publier et partager les résultats 43

5. Suivre les écarts et leur prise en charge 44

Conclusion 46

Liste des annexes 47

Qu'est-ce que le programme Imperium et pourquoi devriez-vous le mettre en place dans votre organisation ?

Toute organisation disposant d'une empreinte numérique incluant des données, de l'infrastructure, des systèmes ou des appareils a la responsabilité de protéger cette empreinte contre la corruption, la compromission ou le vol que ces risques proviennent d'acteurs malveillants ou d'erreurs humaines. Pour y parvenir, les entreprises doivent appliquer les meilleures pratiques de sécurité de l'information et se conformer aux standards de l'industrie, c'est-à-dire mettre en place des contrôles reconnus pour protéger leurs actifs en assurant leur disponibilité, leur intégrité et leur confidentialité et respecter les normes éprouvées.

Malgré cette cible, la posture de sécurité de nombreuses organisations demeure fragile, car elle repose souvent sur des contrôles de sécurité non structurés, non automatisés, ou vérifiés de façon réactive plutôt que proactive. Pour mieux protéger leurs clients et leurs actifs, ces organisations bénéficieraient d'une approche continue, organisée et uniforme entre les entreprises; une méthode standardisée développée par l'industrie, pour l'industrie.

C'est précisément pour adresser ces faiblesses que le programme Imperium a été conçu. Lorsque les étapes de sa mise en place sont pleinement déployées et adoptées, Imperium permet de structurer, fiabiliser et rendre proactif le suivi des contrôles de sécurité d'une organisation. Ce programme implique une évolution des alignements organisationnels afin de mettre un focus sur l'importance de **systématiser** et accélérer notre vérification de l'efficacité de ces contrôles. Elle permet également d'assurer un alignement avec les attentes des régulateurs qui

surveillent les activités de l'entreprise. À ces fins, le programme introduit un processus continu de normalisation, d'évaluation, de revue et d'amélioration des contrôles de sécurité permettant de soutenir la priorisation des efforts et d'assurer une gouvernance durable et moderne.

Les contrôles suivis par Imperium sont identifiés à partir d'un catalogue de contrôles robuste, complet et éprouvé dans l'industrie : le *National Institute of Standards and Technology* (NIST) SP 800-53 v5.2. Le NIST est un référentiel reconnu pour structurer un programme de sécurité de l'information, sélectionner et suivre des contrôles basés sur le risque, s'harmoniser facilement avec la conformité réglementaire et assurer une gestion continue et cohérente de la cybersécurité. Il offre un niveau de détail opérationnel permettant de définir des contrôles précis, mesurables et directement applicables dans les organisations. Ce catalogue permet donc d'établir un tronc commun de contrôles vitaux et nécessaires, applicables à toutes les industries, ainsi qu'un ensemble de contrôles spécifiques et personnalisables au contexte d'affaire et besoins de chaque organisation. Cette deuxième catégorie de contrôles est particulièrement intéressante pour éviter qu'une organisation n'investisse dans des contrôles non adaptés à sa réalité, en l'aidant à orienter ses efforts vers ses priorités stratégiques et ses risques les plus critiques. Pour les grandes organisations, la création de programmes sectoriels permettant de comparer les performances entre secteurs ou entre organisations pourrait s'avérer intéressante. Nous en parlerons plus en détails dans la section *Cadre de contrôle* (page 15).

L'humain a également une place centrale dans le programme Imperium. Le programme est fondé sur un principe de responsabilité partagée par les parties prenantes impliquées qui s'observe durant les activités opérationnelles quotidiennes du programme. Il encourage une évolution des responsabilités et un rehaussement de l'imputabilité des acteurs impliqués. La collaboration est un facteur contextuel essentiel à son succès. Imperium prévoit également des formations ciblées pour les

conseils d'administration et les gestionnaires clés. Cet accompagnement sera discuté plus en détails dans une prochaine version du présent guide.

Dans l'ensemble, Imperium constitue un levier stratégique permettant aux organisations de se positionner parmi les leaders canadiens en gouvernance de sécurité de l'information. Il permet aussi un meilleur étalonnage entre les organisations d'un même secteur d'activités.

Quels sont les facteurs de succès préalables à la mise en place du programme Imperium ?

Avant de débuter la mise en place du programme Imperium dans votre organisation, certains facteurs doivent être considérés pour favoriser une implémentation simple et fluide. Ces facteurs assureront la cohérence, l'efficacité et la continuité du programme. Il s'agit de la création d'une équipe centrale et de la préparation du terrain. La préparation inclut notamment l'obtention du support exécutif, la mobilisation des parties prenantes et l'alignement de votre organisation avec la cible du programme.

1. Création d'une équipe centrale et identification du promoteur exécutif

La première étape est l'identification de l'équipe centrale Imperium. Cette équipe est responsable de préparer le terrain, de mettre en place le programme et d'en assurer la pérennité au sein de l'organisation, notamment en maintenant une

communication régulière avec les exécutifs et les parties prenantes, et en coordonnant l'ensemble des activités du programme. En d'autres-mots, l'équipe centrale est responsable et imputable de la gouvernance et du suivi du programme. En tant que point de contact avec les exécutifs, elle s'assure que le programme reste aligné avec la stratégie de sécurité et les objectifs d'affaires.

Dans cette équipe, deux rôles doivent être identifiés avant de démarrer la mise en place du programme Imperium : un promoteur exécutif et un responsable d'orchestration.

Le promoteur exécutif détient l'imputabilité totale du programme et agit à titre de contact principal avec la haute direction et, si applicable, les membres du conseil d'administration. Son implication continue est essentiel au bon déroulement du programme. Il arbitre les décisions structurantes et donne des orientations en cas d'enjeux majeurs ou de bloquants. Dans les grandes organisations, ce rôle correspond généralement à celui du CISO (Chief Information Security Officer).

Le responsable d'orchestration accompagne le promoteur exécutif. Il est responsable de partager les alignements et les attentes des exécutifs aux autres parties prenantes afin d'assurer la continuité de la vision stratégique. Il est aussi responsable de créer et exécuter une feuille de route qui représente cette vision. Ces responsabilités détaillées sont présentées dans la section *Rôles et responsabilités* (page 10). Dans les grandes organisations, il peut être recommandé d'avoir deux responsables d'orchestration pour se partager la charge de travail selon les forces de chacun.

L'équipe centrale comprend d'autres rôles qui seront impliqués lors de la mise en place du programme. Ils sont présentés dans la section *Rôles et responsabilités* (page 10).

2. La préparation du terrain

La deuxième étape est la préparation du terrain. Cette préparation requiert l'obtention du support exécutif, la mobilisation des équipes et la création d'un plan de déploiement. Elle est réalisée par le promoteur exécutif et le responsable d'orchestration.

Support exécutif

Le support exécutif fait référence à un soutien affirmé et soutenu de la haute direction. Le succès du programme est en effet grandement influencé par cette capacité à engager les exécutifs et, si applicable, les membres du conseil d'administration de l'organisation dès le début des réflexions.

La transformation induite par Imperium exige une implication stratégique et une volonté organisationnelle claire. Ce support exécutif est nécessaire pour trancher les arbitrages entre les risques de sécurité, les besoins d'affaires et les échéanciers, attribuer les ressources adéquates et inscrire Imperium dans la feuille de route globale de l'organisation plutôt que dans un silo technologique. En d'autres-mots, il s'agit d'un levier clé pour influencer les opérations, prendre des décisions et orienter les objectifs d'affaires et les investissements. Concrètement, la mobilisation et le ralliement des exécutifs autour de la valeur d'affaires liée à l'implantation et à la pérennisation du programme Imperium assurent sa légitimité au sein de l'organisation. Selon votre organisation et le plan de déploiement qui sera développé, la montée en maturité du programme s'étalera généralement sur plusieurs mois (voire année), il est donc important que la haute direction demeure des promoteurs engagés tout au long de la démarche. Le promoteur exécutif sera responsable de maintenir cet engagement en rappelant la vision et s'assurant que le programme soit maintenu comme priorité. Dans le cas contraire, l'organisation n'en tirera pas probablement pas les bénéfices escomptés.

La réalisation d'une tournée de présentations exécutives vivantes et engageantes est l'une des techniques les plus efficaces pour obtenir le support exécutif. Pour vous accompagner dans la démarche, une présentation exécutive clé en main sera déposé sur le site de CyberEco prochainement.

L'absence de soutien explicite et en continu de la haute direction conduit souvent à des initiatives de sécurité perçues comme facultatives, à une faible priorisation des chantiers, à des résistances locales non résolues et ultimement à un programme qui peine à livrer ses bénéfices et à être pris au sérieux par les unités d'affaires. Pour ces raisons, il est essentiel d'obtenir le support exécutif avant de démarrer les étapes de la mise en place du programme et de les garder informer tout au long de son implémentation.

Création d'un plan de déploiement

La préparation du terrain fait également référence à la création d'un plan de déploiement, semblable à un plan de projet. Ce plan vise à définir la cadence de déploiement souhaité, les différents jalons à respecter pour atteindre les cibles fixées par l'organisation et la haute direction ainsi que la montée en maturité du programme. L'équipe centrale doit identifier les parties prenantes les plus impactées et/ou les plus prêtes au changement afin de cibler les bonnes audiences à chaque étape de du plan de déploiement. Une entreprise pourrait, par exemple, décider de faire qu'une partie de la transformation durant la première année sur un secteur uniquement afin de tester sa gestion de changement et ses outils avant de l'étendre à tous ses secteurs. Le plan de déploiement doit aussi inclure un recensement des demandes de contribution requises pour l'obtention du financement ou des ressources requises pour la mise ne place du programme.

Mobilisation des parties prenantes

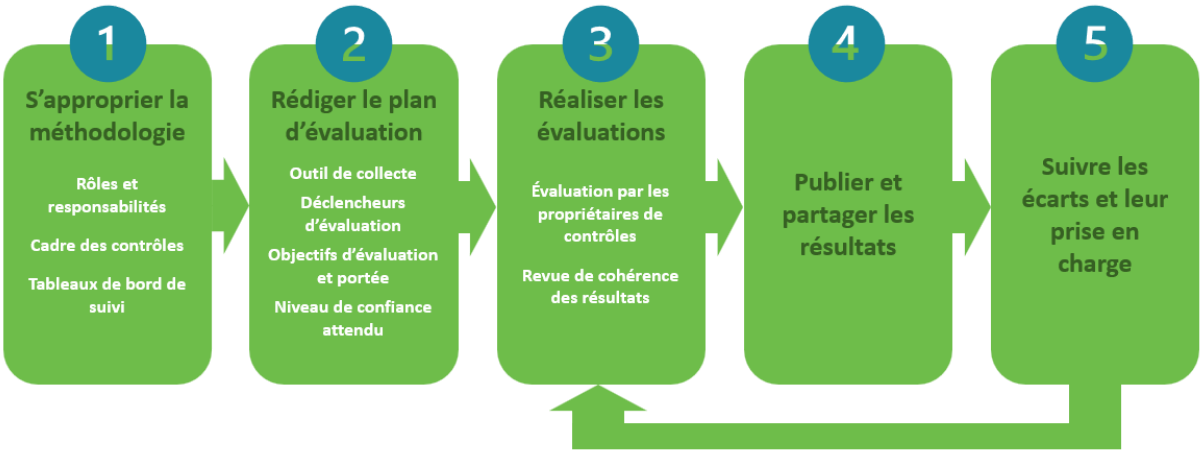
Une fois le support exécutif obtenu, il est important de préparer le terrain pour s'assurer que les prérequis du programme soient en place et que les parties prenantes soient prêtes à s'impliquer dans le changement. Le programme Imperium impliquera, entre-autre, une évolution des rôles, des responsabilités et des processus internes de votre organisation. Cette préparation au changement est une étape primordiale afin de limiter les résistances et favoriser l'engagement des personnes impliquées.

Pour démarrer cette mobilisation, l'une des techniques les plus efficaces est de présenter sommairement la valeur attendue par le programme Imperium aux principaux contributeurs identifiés dans le plan de déploiement. Comme pour les exécutifs, une tournée dans les comités de gestion des équipes, rencontres d'employés ou une présentation dans un format « midi-conférence » sont des tribunes intéressantes pour partager ce message. Une liste des parties prenantes est présentée dans la section *Méthodologie* (page 10).

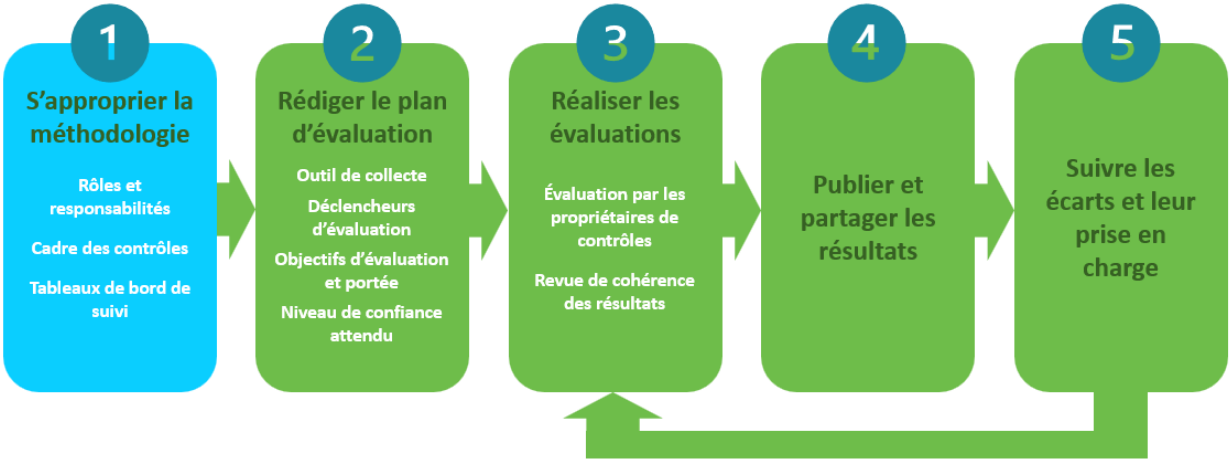
Pour maintenir cette mobilisation, l'équipe centrale sera responsable d'assurer un dialogue structuré et continu avec ses parties prenantes en faisant preuve de transparence quant à la normalisation des processus et méthodes de travail et à la feuille de route d'Imperium. Ces échanges ont pour but de développer un espace collaboratif et de confiance et ainsi d'atteindre la cible du programme.

Quelles sont les étapes de mise en place du programme Imperium ?

La mise en place du programme Imperium repose sur une séquence d'étapes structurées qui permettent de s'approprier la méthodologie définie par le standard d'industrie CyberEco, de créer le cadre des contrôles de sécurité de l'information à évaluer, de mettre en place les outils et les mécanismes de suivi nécessaires, puis de réaliser les évaluations requises. Les étapes sont présentées dans le visuel suivant.



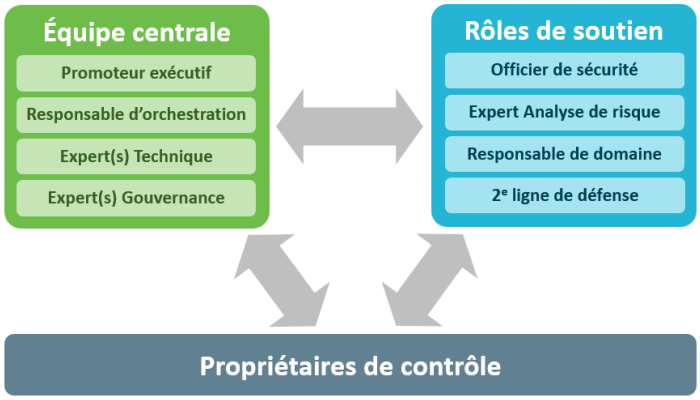
1. S'approprier la méthodologie



La méthodologie décrit le fonctionnement opérationnel du programme Imperium et les fondements qui rendent le programme structuré et reproductible. Ce chapitre comprend la définition des rôles et responsabilités à attribuer, la création du cadre de contrôle propre à votre secteur d'activité et la création des tableaux de bord.

Rôles et responsabilités

Un facteur clé pour le succès du programme Imperium est l'attribution des rôles et responsabilités aux personnes ayant la capacité et la légitimité de les incarner dans l'organisation. Elle favorise la collaboration fluide entre les acteurs qui conçoivent le programme, qui le dirigent, qui le font vivre au quotidien et qui détiennent la responsabilité opérationnelle des contrôles. Imperium regroupe ces rôles en trois grandes catégories : l'équipe centrale, les propriétaires de contrôles et les rôles de soutien.



L'équipe centrale : gouvernance et suivi du programme

Tel que présenté dans la section sur les facteurs de succès préalable, l'équipe centrale est responsable de la gouvernance et du suivi du programme. Elle assure l'alignement avec la stratégie de sécurité globale de l'organisation et les objectifs d'affaires. Elle met en place également la méthodologie et assure le suivi des mécanismes d'évolution au fil des cycles du programme. Cette équipe inclut un promoteur exécutif (décrit dans la section précédente), un responsable d'orchestration et différents experts.

Le responsable d'orchestration accompagne le promoteur exécutif. Il est responsable de partager les attentes des exécutifs aux autres parties prenantes afin d'assurer la continuité de la vision stratégique. Il est aussi responsable de créer et exécuter une feuille de route qui représente cette vision. Dans les grandes organisations, il peut être recommandé d'avoir deux responsables d'orchestration pour se partager la charge de travail selon les forces de chacun. Ces responsabilités incluent notamment :

- Former le reste de l'équipe centrale qui va l'appuyer dans ses tâches quotidiennes
- Réaliser la gestion de changement auprès des parties prenantes et des équipes impactées durant les différentes étapes de la mise en place

- S'approprier la méthodologie en se basant sur le standard Imperium proposée par CyberEco
- Coordonner les activités régulières du programme
- Définir et exécuter la feuille de route et les évolutions du programme Imperium (évolutions basées sur la montée en maturité du programme dans l'organisation et sur les évolutions du standard Imperium définit par l'industrie via CyberEco)
- Définir et faire les demandes pour obtenir les ressources nécessaires au bon fonctionnement (humaines, monétaires, systèmes)
- Rendre compte des résultats d'Imperium et de la performance opérationnelle des parties prenantes

L'équipe centrale regroupe aussi des experts, souvent déjà présents dans l'organisation, essentiels au fonctionnement du programme. Ces personnes contribuent à la création et à la documentation de la méthodologie, à l'analyse des résultats et à la cohérence des interprétations, ainsi qu'à l'accompagnement des parties prenantes. Certains possèdent une expertise technique liée aux plateformes de collecte ou de visualisation, tandis que d'autres contribuent davantage à la gouvernance, à la formation ou à l'accompagnement. Les responsabilités à couvrir sont :

- Adapter, si besoin, la méthodologie, les processus et les procédures proposés dans le standard Imperium de CyberEco
- Accompagner les parties prenantes dans la réalisation des évaluations
- Valider les données collectées pour s'assurer de leur qualité
- Choisir l'outil de collecte des données d'évaluations (page 28)
- Créer des tableaux de bord de suivi des résultats (page 22)
- Partager le résultat des évaluations (page 36)
- Suivre les écarts et assurer leur prise en charge (page 37)

Ainsi, l'équipe centrale est constituée de rôles variés. Sa taille et sa composition évoluent selon la complexité de l'organisation, mais son objectif demeure constant : assurer une gouvernance cohérente, durable et crédible du programme Imperium. Elle n'a pas la responsabilité de réaliser les évaluations : elle accompagne les parties prenantes dans cette activité.

Les propriétaires de contrôles : responsabilité opérationnelle

Puisqu'Imperium a comme objectif de suivre l'efficacité des contrôles de sécurité de l'information, il est essentiel d'identifier un répondant pour chacun de ces contrôles. Ce rôle est nommé « propriétaire de contrôle ». Il est fortement recommandé d'identifier des propriétaires de contrôle ayant une position hiérarchique de gestion dans l'organisation afin d'appuyer la notion d'imputabilité associé à ce rôle. La personne sera ainsi légitimée lorsqu'elle endossera l'évaluation du contrôle.

Le propriétaire de contrôle est la personne dans l'organisation qui connait et maîtrise le contrôle : il est imputable de sa mise en œuvre, de son maintien, de sa couverture et de sa disponibilité. Il est donc le mieux placé pour démontrer l'efficacité de ce contrôle. Il est important de retenir qu'un contrôle peut prendre différentes formes : il peut être un processus, un outil, un système ou même un humain.

Le propriétaire participe activement aux évaluations du (ou des) contrôle(s) sous sa responsabilité : il fournit l'information requise en confirmant si le contrôle est déployé conformément aux objectifs d'évaluation et met à disposition les éléments de preuve attendus. Il est également responsable de justifier les écarts observés et de les prendre en charge. Le propriétaire peut déléguer à un répondant, mais demeure imputable de la complétude et de la qualité des informations.

Si votre organisation n'a pas déjà un registre des propriétaires de ses contrôles de sécurité de l'information, il est grandement utile d'attendre la définition de votre cadre de contrôle pour les identifier. Dans ce contexte, différentes techniques peuvent être utilisées pour identifier les propriétaires de contrôle. Deux techniques sont présentées dans ce guide. La première technique est l'utilisation des registres actuellement en place dans l'organisation pour associer les contrôles aux propriétaires d'affaires des différents processus et outils technologiques de l'organisation. L'équipe centrale est responsable de faire cette association puisqu'elle a le niveau de connaissance le plus élevé du cadre de contrôle. Une fois cet exercice terminé, les contrôles sans propriétaire devront être examinés un à un avec les différentes équipes de sécurité pour en déterminer le propriétaire adéquat. La deuxième technique est plus appropriée pour une organisation qui n'a pas de registre de propriétaire d'affaires. Elle peut également être utilisée en complément à la première technique afin d'identifier les propriétaires de contrôles manquants. Elle consiste a identifier des *Responsables de domaines*. L'objectif est de classer les contrôles par grands domaines – gestion des identités et des accès, sécurité applicative, réponse aux incidents, etc. – puis d'attribuer un responsable de domaine à chacun (deux listes de domaine sont disponibles à l'Annexe 1 pour inspiration). L'équipe centrale fait le lien entre les contrôles et les domaines. Le responsable prendra ensuite le temps nécessaire pour identifier le propriétaire adéquat pour chaque contrôle de son domaine. Cette approche permet aussi de constituer un réseau rapproché autour de l'équipe centrale, facilitant la communication : l'équipe centrale transmet les messages au responsable de domaine, qui les partage ensuite aux propriétaires, au besoin.

Les rôles de soutien : pilotage et suivi continu

Les rôles de soutien sont facultatifs au bon fonctionnement du programme Imperium. Ils sont présentés dans ce guide à titre indicatif pour les organisations de plus grande taille, qui doivent généralement composer avec de vastes équipes et des secteurs d'affaires aux réalités et priorités distinctes. De façon générale, ces personnes agissent comme intermédiaires entre l'équipe centrale et différentes équipes dans l'organisation.

L'un des acteurs pouvant jouer ce rôle est l'officier de sécurité (équivalent au BSO (Business Security Officer) ou BISO (Business Information Security Officer)). Cet acteur facilite l'alignement entre la sécurité et les secteurs d'affaires d'une grande organisation. Il accompagne les dirigeants des secteurs d'affaires dans la priorisation de leurs investissements et les aide à prendre des décisions à travers des recommandations liés à leurs risques ou problématiques de sécurité. L'officier de sécurité est donc un acteur particulièrement pertinent à inclure dans le programme Imperium, puisqu'il agira comme porte-parole des résultats liés aux contrôles de sécurité propres aux secteurs. En complément, il peut aider dans le pilotage des cycles d'évaluation et suivre la réalisation des évaluations en restant informé de l'avancement des collectes et de la prise en charge des écarts.

Le responsable des analyses de risque occupe un rôle de soutien essentiel, à forte valeur ajoutée. Cette personne peut contribuer à contextualiser et vulgariser les résultats et ainsi partager les résultats dans un langage clair et accessible pour les exécutifs.

Le responsable de domaine présenté précédemment constitue également un bon exemple de rôle de soutien pour accompagner l'équipe centrale.

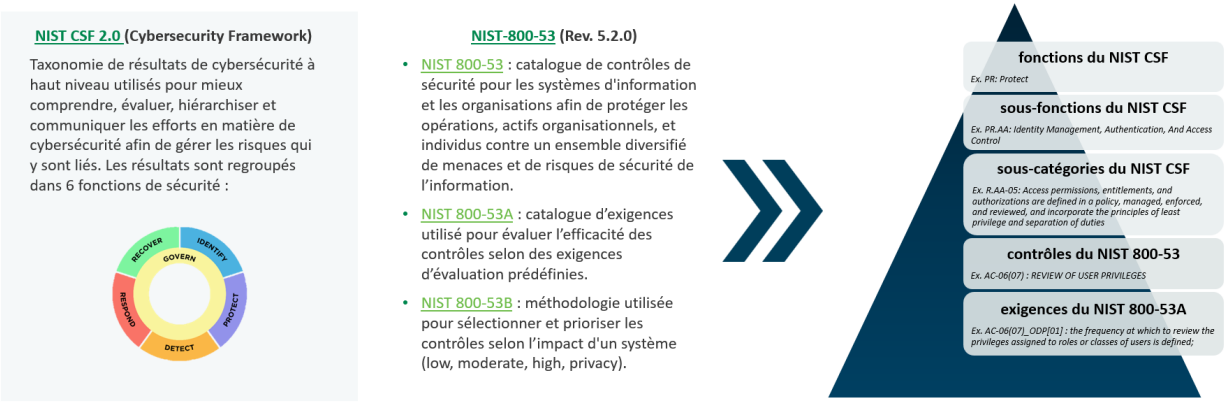
Enfin, au sein des organisations plus vastes ou soumises à une forte réglementation, le concept de lignes de défense est généralement déjà en place.

L'évaluation des contrôles est réalisée par la première ligne de défense, tandis que la deuxième ligne intervient pour renforcer l'assurance qualité de ces évaluations. Elle mène des revues indépendantes ciblées, ce qui augmente la confiance dans les résultats et renforce leur crédibilité auprès des auditeurs et des régulateurs.

Cadre de contrôles

Le cadre de contrôles correspond à la liste de tous les contrôles que l'organisation doit implémenter pour répondre à ses besoins de sécurité. À cette liste doivent être ajoutés les noms des propriétaires de chaque contrôle. Cette information est essentielle pour atteindre l'objectif du programme Imperium, qui consiste à systématiser et accélérer l'évaluation des contrôles afin de démontrer leur efficacité et de fournir une visibilité claire sur la posture de sécurité de l'organisation.

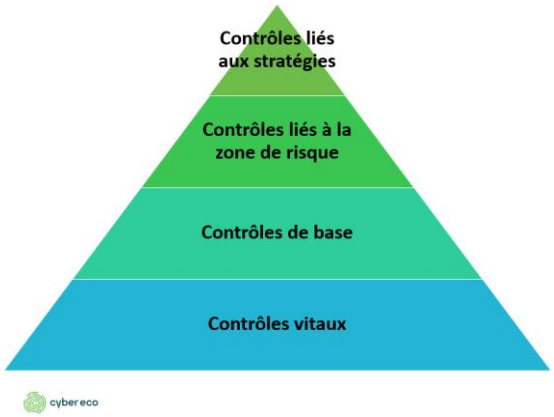
Afin d'avoir un cadre de contrôles de sécurité précis, exhaustif et aligné sur des pratiques reconnues, Imperium se base sur les cadres de références du NIST. Plus spécifiquement, le cadre NIST SP 800-53A rev5.2, qui fournit les procédures d'évaluation des contrôles de sécurité ainsi que le cadre NIST SP 800-53B rev5.2, qui fournit une méthodologie permettant de choisir et de prioriser les contrôles basés sur le niveau d'impact des actifs technologiques sur la sécurité. La figure suivante présente plus en détails les différents cadres du NIST. L'équipe centrale se doit de bien les comprendre afin de pouvoir les expliquer aux parties prenantes du programme.



Dans les grandes organisations aux champs d'activités diversifiés, il est fortement recommandé de créer des cadres de contrôles propres à chaque secteur d'activités afin de refléter adéquatement leur réalité et les obligations réglementaires qui les régissent. Cet exercice permet un alignement juste quant aux investissements et priorités et chacun. Par souci de simplicité, il est également possible de le faire dans une deuxième phase de la mise en place du programme Imperium.

Comprendre les niveaux de contrôles

Imperium utilise quatre niveaux de priorisation pour catégoriser les contrôles du NIST SP 800-53 rev5.2. Ces niveaux permettent de définir les contrôles applicables à toutes les organisations et des contrôles spécifiques à la réalité de chacun.



Le premier niveau de priorisation fait référence aux **contrôles vitaux**. Ces contrôles sont indispensables à la sécurité de l'organisation et constituent le socle minimal attendu pour se protéger des cybermenaces les plus fréquentes. Ces contrôles sont obligatoires et sont les mêmes pour toutes les organisations, indépendamment de leurs secteurs d'activités. L'absence ou l'inefficacité de ces contrôles peut entraîner des conséquences sévères, telles que des incidents majeurs de sécurité, des pertes de données critiques, des sanctions réglementaires ou des impacts significatifs sur la continuité des activités.

Le deuxième niveau de priorisation fait référence aux **contrôles de base**. Ces contrôles sont nécessaires à une posture solide et stable. Ils permettent de soutenir la conformité aux normes et réglementations et maintenir la stabilité opérationnelle. Ces contrôles sont obligatoires. Leur absence ou leur inefficacité peut engendrer des perturbations opérationnelles, une perte de confiance des clients, des sanctions réglementaires et des pénalités financières.

Le troisième niveau de priorisation fait référence aux **contrôles liés à la zone de risque**. Ces contrôles renforcent les niveaux précédents en ciblant des contrôles permettant de réduire l'impact ou la probabilité d'un incident. Pour les sélectionner, l'organisation doit identifier les scénarios de risque de sécurité de l'information

propres à son secteur d'activité. Ces contrôles ne sont pas obligatoires, mais fortement recommandés pour mitiger ces risques.

Le quatrième niveau de priorisation fait référence aux **contrôles liés aux stratégies** de l'organisation. Ces contrôles visent une posture d'excellence en sécurité de l'information, au-delà des objectifs minimaux et obligatoires. Ils soutiennent l'innovation, l'anticipation des menaces émergentes et l'alignement avec les orientations stratégiques de l'organisation. Ces contrôles ne sont pas obligatoires, mais fortement recommandés pour atteindre les objectifs stratégiques de l'entreprise. Leur absence n'entraîne pas nécessairement une non-conformité immédiate, mais peut compromettre la capacité de l'organisation à se positionner comme un leader en matière de sécurité de l'information.

La compréhension de ces niveaux de priorisation par l'ensemble des parties prenantes est essentielle pour assurer un alignement stratégique partagé. Cet alignement permettra de donner un sens aux priorités et aux investissements, évitant ainsi de les orienter sur des systèmes ayant plus de visibilité ou des projets médiatisés, au détriment d'enjeux moins visibles, mais essentiels pour la posture de sécurité de l'organisation.

Identifier et prioriser les contrôles à l'aide de l'arbre décisionnel Imperium

En complément à la définition de ces quatre niveaux de priorisation, Imperium facilite la sélection des contrôles en vous offrant une méthode standardisée, qui favorise une comparaison entre les organisations. Un arbre décisionnel est utilisé pour sélectionner les contrôles à implémenter et à évaluer en les classant dans les quatre niveaux de priorisation discutés précédemment. Cet arbre décisionnel permet donc de créer une liste de contrôles de sécurité de l'information justifiée et

proportionnée, alignée sur le contexte d'affaires et le profil de risque de l'organisation.

Bien connaître son écosystème

Pour être capable de prendre des décisions éclairées quant aux contrôles à implémenter dans une organisation, il est essentiel de disposer d'un inventaire suffisamment fiable des systèmes et des processus de l'organisation ainsi que de leur impact (ou criticité). L'impact réfère au niveau de disponibilité, de confidentialité et d'intégrité requis pour que l'organisation opère correctement. Plus ce niveau est élevé, plus le système est critique pour l'organisation et doit être protégé. L'inventaire permettra de contextualiser où et quand un contrôle doit être appliqué afin d'éviter de surinvestir en appliquant systématiquement les contrôles de manière transverse.

Il demeure possible pour une organisation de débuter Imperium en suivant une approche « transverse »; tous les contrôles sur tous les systèmes. Cependant, cette organisation voudra rapidement rationnaliser davantage ses investissements à l'aide d'un inventaire.

Débuter l'identification et la priorisation

Pour débuter, l'organisation part du catalogue de contrôle complet du NIST SP 800-53A rev5.2 (disponible sur le site officiel du NIST) et suit l'arbre décisionnel afin de ne conserver que les contrôles qui s'appliquent. Les étapes de l'arbre décisionnel sont expliquées dans ce chapitre. Le visuel de l'arbre décisionnel est disponible en grande taille à l'Annexe 2.

Les baselines du NIST SP 800-53 rev5.2

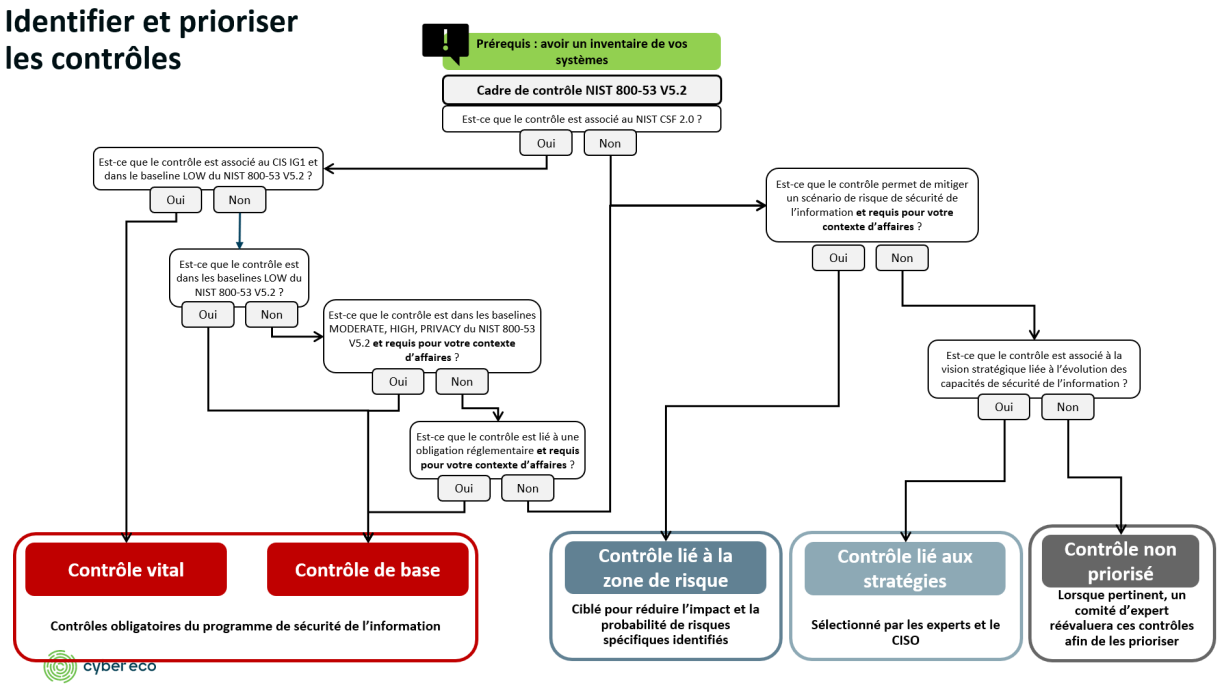
L'arbre décisionnel Imperium fait référence à des *baselines* utilisées dans le NIST SP 800-53 rev.5.2. Les *baselines* sont des profils de référence standardisés qui

indiquent quels contrôles minimaux doivent être mis en place selon le niveau d'impact d'un système.

Le NIST propose trois *baselines* principales :

- **Low baseline** – pour les systèmes à faible impact
- **Moderate baseline** – pour les systèmes à impact modéré
- **High baseline** – pour les systèmes à fort impact
- **Privacy baseline** – pour les systèmes qui entreposent ou partagent des renseignements personnels.

Ces *baselines* sont disponibles dans le catalogue complet du NIST SP 800-53 rev5.2.



L'**identification des contrôles vitaux** est le premier chemin à suivre. Ces contrôles constituent la fondation sur laquelle aucune organisation ne peut faire l'impasse pour maintenir une posture de sécurité de l'information viable. Ils ont été identifiés en

consolidant les connaissances de trois référentiels complémentaires ayant fait leur preuve dans l'industrie : le *NIST Cybersecurity Framework 2.0* (NIST CSF 2.0), le *Center for Internet Security Controls Implementation Group 1* (CIS IG1) et la *baseline* LOW du NIST SP 800-53 rev5.2. Cette combinaison permet d'identifier 40 contrôles vitaux. Comme ils sont identiques pour l'ensemble des organisations, cette liste est présentée à l'Annexe 3.

L'**identification des contrôles de base** est le deuxième chemin à suivre. Ces contrôles comprennent un tronc commun applicable à toutes les organisations (les contrôles de la *baseline* LOW du NIST 800-53 rev. 5.2 n'étant pas considérés comme des contrôles vitaux), ainsi qu'un ensemble de contrôles spécifiques à chaque organisation ou à chacune de ses entités. En effet, lorsque mentionné dans l'arbre décisionnel, le contexte d'affaires de l'organisation et de ses entités/secteurs doivent être considérés afin de prendre des décisions liées à sa réalité spécifique. Par exemple, un contrôle peut être lié à une obligation réglementaire pour un secteur seulement.

Pour répondre à la question : « Le contrôle figure-t-il dans les baselines *MODERATE*, *HIGH* ou *PRIVACY* du NIST 800-53 v5.2 et est-il requis pour votre contexte d'affaires ? », l'équipe centrale doit consulter l'inventaire des systèmes de l'organisation. Si l'organisation ou le secteur ciblé par le cadre de contrôle a :

- Au moins un système ayant un impact modéré sur l'organisation, elle doit conserver tous les contrôles de la *baseline* MODERATE
- Au moins un système ayant un impact élevé sur l'organisation, elle doit conserver tous les contrôles de la *baseline* HIGH
- Au moins un système permettant d'entreposer ou de partager des renseignements personnels, elle doit conserver tous les contrôles de la *baseline* PRIVACY

Le fait de devoir implémenter et évaluer ces contrôles sur un système ou non sera expliqué plus en détail dans la section *Réaliser l'évaluation* (page 33).

Pour répondre à la question « Est-ce que le contrôle est lié à une obligation réglementaire et est requis pour votre contexte d'affaires ? », l'équipe centrale doit connaître l'ensemble des obligations réglementaires que l'organisation doit respecter. Un exemple est la nécessité de respecter des certifications ISO ou la conformité SOX en gestion des identités et des accès. Certains de ces cadres réglementaires offrent l'association entre leur requis et les contrôles du NIST SP 800-53 rev5.2. Dans le cas contraire, l'équipe centrale devra prendre le temps de réaliser manuellement l'association. Les entreprises membres de CyberEco vont travailler sur ces associations afin d'accompagner davantage les organisations voulant adhérer à Imperium. Ce contenu sera disponible dans une prochaine version de ce guide.

L'**identification des contrôles liés à la zone de risque** est le troisième chemin à suivre. Ces contrôles sont sélectionnés en considérant les scénarios de risque de sécurité de l'information spécifiques à votre organisation. L'idée est d'identifier les contrôles principaux qui permettent de mitiger ces scénarios. Afin de simplifier la tâche, Imperium offre une liste de scénarios de risques prédéfinis à l'aide des entreprises membres de CyberEco et les contrôles qui y sont associés. Votre organisation peut ainsi partir de cette liste de contrôles et l'ajuster au besoin. Tous les contrôles qui ne sont pas déjà dans le niveau de priorisation « vital » ou « de base » iront dans ce niveau. La liste est disponible à l'Annexe 4.

L'**identification des contrôles liés aux stratégies** est le quatrième chemin à suivre. Pour les identifier il est recommandé de partir du plan stratégique de votre organisation, de votre équipe de technologie de l'information ou de votre équipe de sécurité. À partir de ces plans stratégiques, des ateliers avec le Chef de la sécurité de

l'information et ses experts doivent être réalisés afin de préciser la vision stratégique long terme de sécurité de l'information. Une fois les stratégies spécifiques à la sécurité de l'information identifiées, il sera possible de les associer à des contrôles du NIST SP 800-53 rev5.2 qui ne sont pas déjà inclus dans les trois premiers niveaux de priorisation. Ces contrôles visent ainsi une posture d'excellence et de leader dans l'industrie.

Le dernier chemin représente les contrôles **non priorisés**. Ces contrôles devront être documentés et réévalués lorsqu'un déclencheur est activé (page 28).

En conclusion, cet exercice d'identification et de priorisation permet créer le cadre de contrôles de votre organisation en vous assurant qu'il est cohérent à la fois avec le standard Imperium de l'industrie et avec la réalité opérationnelle de l'organisation. Elle garantit que chaque contrôle retenu contribue directement à la réduction des risques, à la conformité et à l'atteinte des objectifs d'affaires, tout en offrant la flexibilité nécessaire pour faire évoluer le cadre au fil du temps alors que les menaces, les technologies et les priorités changent.

Tableaux de bord de suivi

L'appropriation de la méthodologie Imperium passe ensuite par le développement de l'outil servant à partager les résultats de l'évaluation des contrôles aux parties intéressées. La création d'un tableau de bord est la technique recommandée pour présenter visuellement ces résultats et les rendre accessible à tous. Il permettra de soutenir une saine prise de décision en acheminant l'information de sécurité au bon niveau hiérarchique, au bon moment et de manière appropriée.

En effet, le tableau de bord n'est pas seulement un rapport informatif, il supporte la gouvernance, alimente le dialogue entre équipes et aide à la prise de décision quant aux investissements et aux priorités. Sa structure doit être pensée avant de réaliser les évaluations, car elle influence les champs à collecter et la granularité d'information nécessaire. La qualité des données présentées sur le tableau de bord dépend directement de la rigueur des mécanismes de collecte. Le visuel et le contenu pourront naturellement évoluer selon les commentaires reçus par les consommateurs.

Le tableau de bord permet aussi de donner de la visibilité sur les seuils et les cibles définis par les exécutifs quant à la tolérance au risque de l'organisation. Par exemple, une organisation pourrait se fixer comme objectif d'atteindre 100 % d'efficacité pour ses contrôles vitaux et 75 % pour ceux liés à ses stratégies.

Les types de tableaux de bord de suivi et leurs sections

Deux types de tableaux de bord doivent être développés : un pour le suivi de la mise en place du programme dans l'organisation et un pour le suivi des résultats des évaluations. Le premier est principalement destiné à l'équipe cœur et devient généralement obsolète une fois le programme mis en place. Le deuxième, le tableau de bord de suivi des résultats, est décliné en trois vues complémentaires permettant de répondre aux besoins des différents publics cibles auxquels il s'adresse.

1. La **vue exécutive** est destinée à la haute direction. Cette vue présente la posture de sécurité de l'information globale de l'organisation.
2. La **vue détaillée** est destinée à la haute direction et aux parties prenantes principales du programme Imperium. Elle présente, de façon détaillée, le résultat des contrôles évalués en les divisant en grandes catégories de contrôles.

3. La **vue granulaire** est destinée aux propriétaires de contrôles et aux équipes opérationnelles. Elle présente le résultat des évaluations unitaires.

Pour présenter l'information sous différents angles, des filtres doivent être intégrés aux différentes vues :

- Niveau de priorisation des contrôles
  - Vital
  - De base
  - Zone de risque
  - Lié aux stratégies
- Niveau de confiance des évaluations
  - Auto-évaluation
  - Évaluation revue à l'interne
  - Évaluation revue à l'externe
- Portée d'évaluation :
  - Type d'applications (ex. : applications critiques, joyaux de la couronne)
  - Type d'environnement (ex. : infonuagique ou traditionnel)
- Domaine de sécurité de l'information
  - Voir Annexe 1 pour inspiration
- Cadre de conformité
  - Par exemple : SOC1, PCI-DSS

Certaines organisations tireraient avantage à intégrer des filtres afin d'adapter les vues aux besoins de leurs différents publics cibles. Cela permet de voir l'ensemble des contrôles qui impactent leurs processus d'affaires et leurs systèmes spécifiques.

Les indicateurs à intégrer

Le programme Imperium recommande d'intégrer tous les indicateurs des tableaux suivants dans les tableaux de bord d'une organisation. Il est possible de le faire progressivement, au fur et à mesure que la montée en maturité du programme augmente.

Indicateurs de suivi de la mise en place du programme
Indicateurs liés à la création du cadre de contrôle :

- % d'avancement de l'identification des contrôles obligatoires (vitaux et de base)
    - *Le résultat pour les contrôles vitaux sera à 100% comme la liste est dans le présent guide (Annexe 3)*
- # de contrôles présent dans le cadre de contrôle (par niveau de priorisation)
- % de contrôles ayant un propriétaire de contrôle identifié (par niveau de priorisation)

Indicateur lié à la préparation aux évaluations

- % de contrôles étant prêt pour une évaluation par son propriétaire
    - *Les critères pour être prêt sont :*
        - Propriétaire de contrôle identifié
        - Objectifs d'évaluation (exigences) validés (*voir section Objectifs d'évaluation et portée (page 30)*
        - Portée d'évaluation confirmé (*voir section Objectifs d'évaluation et portée (page 30)*
        - Niveau de confiance attendu confirmé (*voir section Niveau de confiance attendu (page 32)*)
        - Facultatif | Type de collecte confirmé (manuelle ou automatique)
        - Facultatif | Délai attendu pour évaluation confirmé
        - Facultatif | Délai de validité du résultat confirmé

Indicateurs sur le premier cycle d'évaluation des contrôles :

- % de contrôles évalués
    - *Un contrôle est évalué lorsque toutes ses exigences sont évaluées*
- % d'exigences évaluées
- Facultatif | % de contrôles évalués dans les délais attendu

Indicateurs de suivi des résultats des évaluations

• % de satisfaction des exigences qui composent une fonction du NIST-CSF 2.0
  o *Cet indicateur présente l'agrégation la plus large à l'attention de la haute direction. Il permet de démontrer à haut niveau la posture de sécurité de l'organisation à travers les 6 fonctions de sécurité; gouverner, identifier, protéger, détecter, répondre et remédier.*
• % de satisfaction des exigences qui composent les sous-fonctions du NIST-CSF 2.0
  o *Cet indicateur présente une agrégation intéressante autant pour la haute direction que les différentes parties prenantes du programme. Il permet de démontrer la posture de sécurité de*

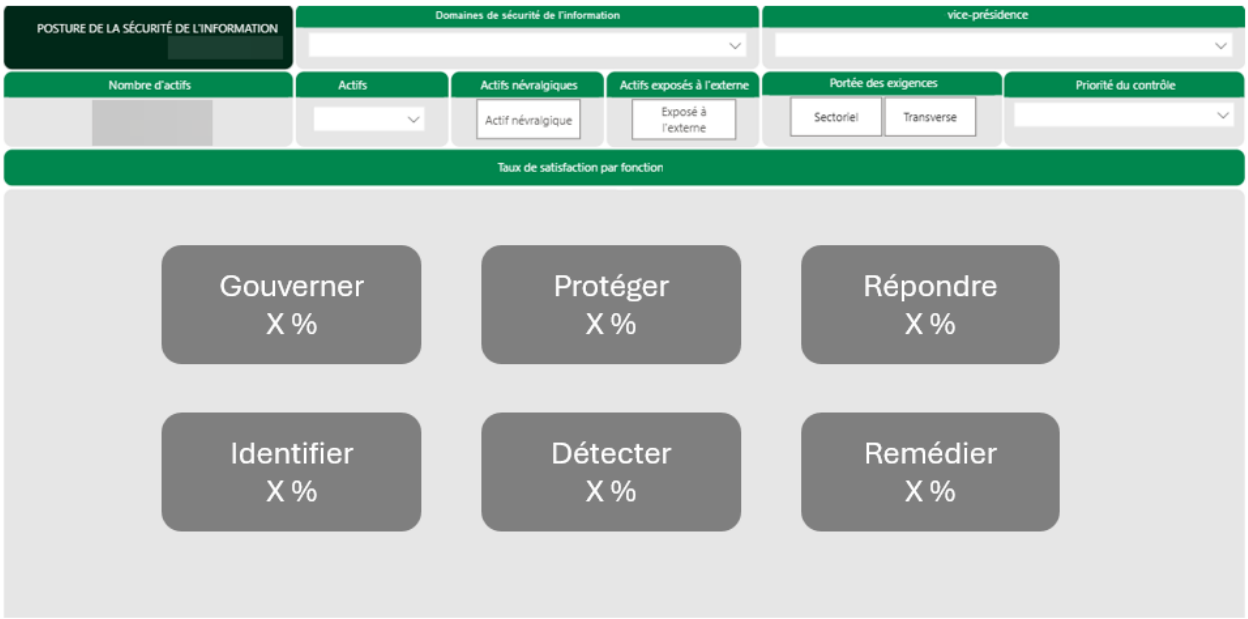
l'organisation à travers les 19 sous-fonctions de sécurité du NIST CSF 2.0. Cet indicateur est utile pour orienter les investissements par la représentation des forces et des faiblesses de l'organisation.

- % de satisfaction des exigences qui composent un contrôle (c'est-à-dire la posture du contrôle)
    - *Cet indicateur plus granulaire est intéressant pour les propriétaires de contrôles et les équipes opérationnelles. Il présente pour chaque contrôle l'agrégation du résultat de ses exigences.*
- % de satisfaction d'une exigence

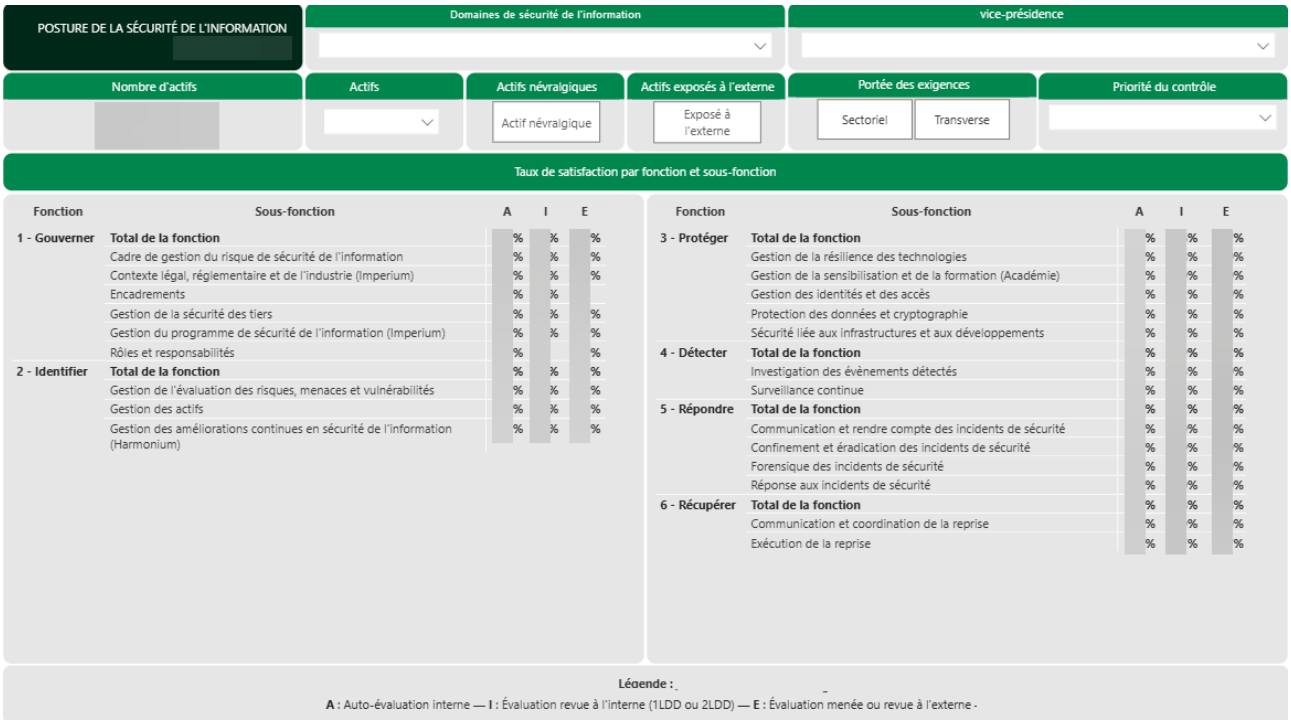
Exemples de maquette

Afin de simplifier la compréhension par les différents publics, il est recommandé de se baser sur des visuels qui sont déjà reconnus dans l'organisation. Voici des exemples de maquettes à titre d'inspiration.

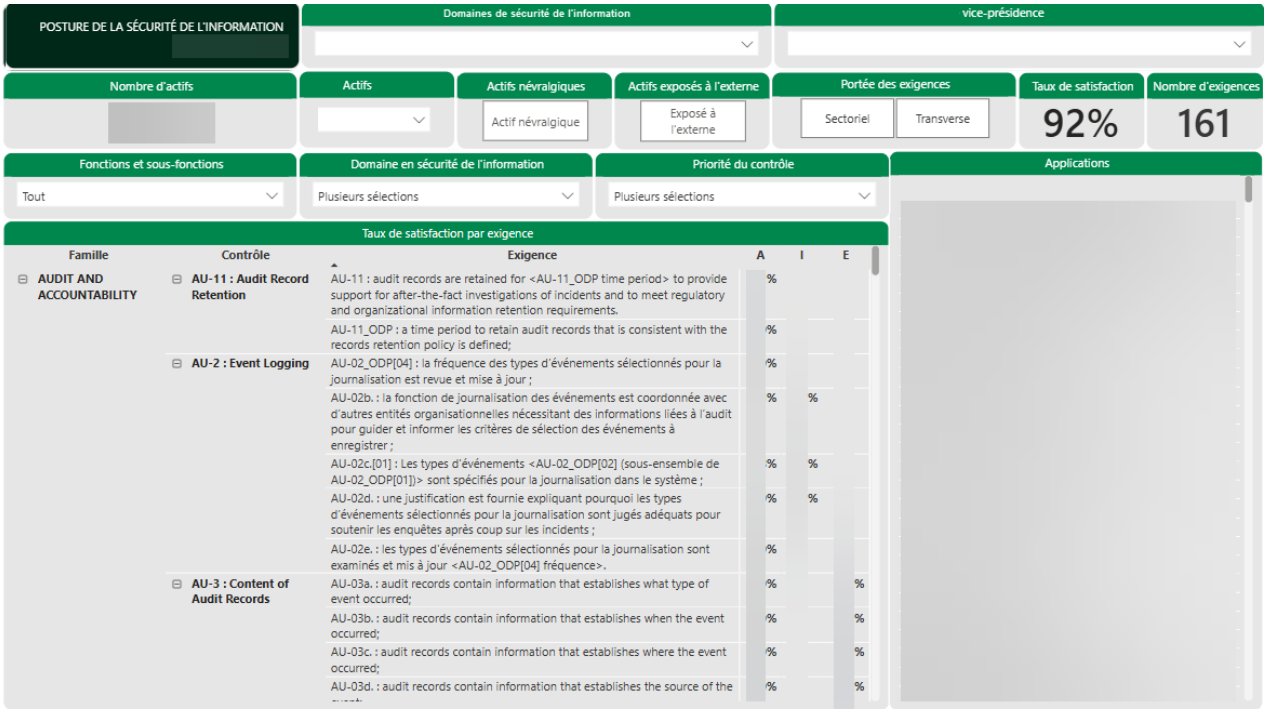
Vue exécutive



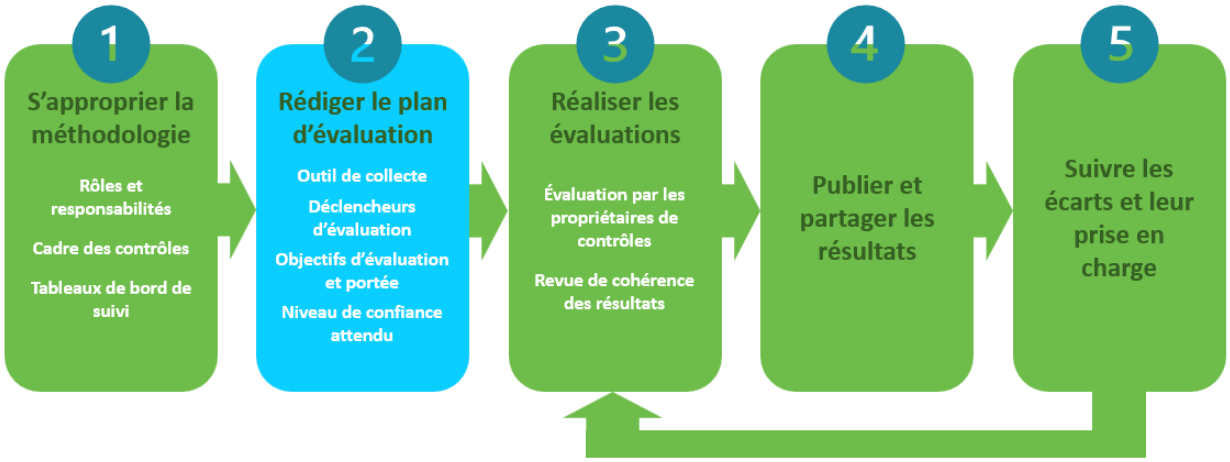
Vue détaillée



Vue granulaire



2. Rédiger le plan d'évaluation



Le plan d'évaluation traduit la méthodologie en planification concrète. Il vise à encadrer le processus de réalisation des évaluations des contrôles. Il doit inclure :

- Le choix de l'outil de collecte;
- La liste des déclencheurs d'une évaluation;
- La portée d'évaluation;
- Les objectifs d'évaluation;
- Le niveau de confiance attendu.

Le concept de déclencheur d'une évaluation est utilisé afin d'assurer une approche dynamique et continue de la révision de la posture de sécurité de l'organisation plutôt qu'une fréquence fixe (ex.: mensuellement, trimestriellement ou annuellement).

Le premier cycle d'évaluation s'étend sur une plus grande période, car il permet de confirmer si les contrôles ciblés sont bien compris et expliqués, s'ils sont applicables sur l'ensemble des portées et si les intrants d'évaluation doivent être collectés

manuellement ou de façon automatisée. Les cycles d'évaluation suivants sont ainsi plus rapides.

Outil de collecte

L'outil de collecte sert à recueillir toutes les informations nécessaires à l'évaluation d'un contrôle. Il servira d'intrant des tableaux de bord de présentation des résultats. Il est possible de démarrer avec des outils simples, puis de renforcer progressivement l'outillage à mesure que le programme gagne en maturité.

Un tableau Excel peut suffire pour structurer une première collecte en l'accompagnant d'un répertoire sécuritaire et partagé tel qu'une plateforme collaborative (ex. SharePoint ou équivalent) pour centraliser les preuves d'évaluation, gérer les versions, contrôler les accès et faciliter la collaboration. Bien que ces outils offrent peu d'automatisation, ils présentent l'avantage d'être accessibles et rapides à mettre en œuvre.

À mesure que les besoins de traçabilité, de contrôle qualité et d'automatisation augmentent, un outil spécialisé de type GRC/IRM (ex. ServiceNow IRM ou équivalent) devient un levier majeur. Il permet d'orchestrer les évaluations, d'assigner des tâches, de standardiser la structure des réponses attendues, d'intégrer des preuves visuelles et de conserver l'historique des validations, tout en réduisant les manipulations manuelles qui introduisent des erreurs. L'automatisation entre l'outil de collecte et un outil de visualisation des tableaux de bord (ex. PowerBI) accélère aussi grandement la production des tableaux de bord. Cette approche rend possible une posture plus proche du temps réel.

Imperium s'inscrit dans une logique d'amélioration continue : l'organisation peut commencer avec des outils proportionnés à sa maturité, puis raffiner les champs de

collecte, renforcer l'automatisation, simplifier les flux de validation et enrichir les visualisations à chaque cycle.

Le type d'information à collecter sera présenté dans la section *Réaliser l'évaluation* (page 33).

Déclencheurs d'évaluation

Afin de présenter une information juste et représentative de l'efficacité des contrôles, Imperium s'appuie sur des déclencheurs, plutôt que sur un calendrier, pour réaliser l'actualisation des résultats. L'objectif est simple : éviter qu'un contrôle soit représenté comme étant satisfaisant ou non satisfaisant alors que son efficacité ou sa portée a changé.

Selon la situation, les déclencheurs peuvent engendrer une évaluation complète de tous les contrôles ou une évaluation ciblée sur un ou quelques contrôles.

Les déclencheurs d'une nouvelle évaluation sont :

Déclencheur	**Action à prendre**
L'évolution du cadre de contrôles par l'ajout, le retrait ou la modification d'un contrôle pour diverses raisons, notamment : • Nouvelle version du référentiel du NIST SP 800-53 disponible • Évolution d'une obligation règlementaire (impact contrôles de base) • Ajout ou modification d'un scénario de risque de sécurité de l'information ciblant l'organisation (impact contrôles liés à la zone de risque)	1. Mettre à jour le cadre de contrôle 2. Réaliser une première évaluation pour tous les contrôles ajoutés 3. Réviser l'évaluation pour tous les contrôles modifiés

• Modification des stratégies de sécurité de l'information de l'organisation (impact contrôle liés aux stratégies)	
La réception d'un rapport interne ou externe tel que : • Audit interne ou externe • Inspection par un régulateur • Test de sécurité offensive • Post-mortem d'un incident	1. Réviser l'évaluation pour tous les contrôles ciblés par l'évaluation
Un changement opérationnel ayant un impact sur un contrôle de sécurité de l'information, par exemple : • Fin d'un projet • Modification d'un processus • Ajout ou retrait d'un système • Changement de responsabilités • Ajout d'un nouveau système • Ajout d'une portée comme l'acquisition d'une nouvelle entité d'affaires	1. Mettre à jour le cadre de contrôle dans le cas où le propriétaire de contrôle a changé 2. Réviser l'évaluation pour tous les contrôles ciblés par le changement
Un changement dans la qualité des intrants, par exemple : • Une source de preuve manuelle maintenant disponible de façon automatisée • Une source de preuve automatisée dorénavant indisponible	1. Ajuster la méthode de collecte de l'évaluation de tous les contrôles ciblés 2. Réviser l'évaluation pour tous les contrôles ciblés
La prise en charge d'un écart soulevé par Imperium (voir la section *Suivre les écarts et leur prise en charge* (page 37)	1. Réviser l'évaluation pour tous les contrôles ciblés
L'obsolescence d'une évaluation basée sur la durée maximale acceptée par l'organisation pour la mise à jour de l'information CyberEco recommande les délais suivants : • Contrôles vitaux et de base : révision annuelle	2. Réviser l'évaluation des contrôles selon la fréquence maximale établie

• Contrôles liés à la zone de risque et aux stratégies : révision aux deux ans	

De manière générale, tout événement susceptible d'affecter la validité, la portée ou la fiabilité des résultats d'évaluation peut être considéré comme un déclencheur. Cette approche permet de maintenir une posture de sécurité vivante et dynamique, continuellement alignée avec la réalité opérationnelle et le niveau de risque de l'organisation, plutôt que figée dans un cycle d'évaluation fixe.

Objectifs d'évaluation (exigences) et portée

Chaque contrôle de sécurité du cadre de contrôle est associé à un ou plusieurs objectifs d'évaluation. Ces objectifs, désignés comme exigences, permettent au propriétaire du contrôle de juger si celui-ci est satisfaisant. Ces exigences sont tirées du NIST SP 800-53A rev. 5.2, assurant ainsi des évaluations fondées sur une méthode reconnue, reproductible et pleinement traçable. Les organisations peuvent donc utiliser ces exigences telles quelles. Ils ont également la liberté de les ajuster selon leur réalité. Ces ajustements doivent cependant être rigoureusement documentés afin de conserver les justificatifs et de s'assurer de les considérer lors de comparaisons avec d'autres organisations ou lors d'évolution du cadre de contrôle. Une exigence peut également être jugée « non applicable » dans une organisation. Encore une fois, ce raisonnement doit être documenté.

Deux règles simples structurent l'évaluation d'un contrôle et ses exigences :

- Une exigence est considérée évaluée lorsqu'une constatation claire a été formulée et validée par le propriétaire du contrôle (ou son répondant), selon la portée applicable.

- Un contrôle est considéré évalué lorsque l'ensemble de ses exigences applicables sont évaluées et validées par son responsable (ex. l'équipe d'orchestration, le propriétaire de contrôle).

La figure suivante présente un exemple. Le *AT-04 Training Records* est le contrôle. Ce contrôle doit respecter 4 exigences pour être satisfaisant.

AT-04 TRAINING RECORDS

SP 800-53A Assessment Objectives

Determine If	
AT-04_ODP	time period for retaining individual training records is defined;
DS-AT-04a.[01]	information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training, are documented;
DS-AT-04a.[02]	information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training, are monitored;
DS-AT-04b.	individual training records are retained for AT-04_ODP time period.

L'outil de collecte Imperium doit ainsi prévoir un champ pour présenter et collecter les informations suivantes :

- Le nom et le numéro du contrôle
- Le statut d'évaluation pour chaque exigence qui sera saisie par le propriétaire de contrôle. Les options recommandées par le NIST sont : satisfaisant, autre que satisfaisant et non applicable.
- Un commentaire qualitatif saisit par le propriétaire de contrôle permettant d'expliquer des particularités, de documenter des hypothèses, et de soutenir la collecte d'évidences.

En plus des exigences à respecter, l'évaluation d'un contrôle est influencée par la portée qu'il couvre. La portée, aussi appelée la couverture, réfère à l'endroit où un contrôle doit être implémenté et évalué. Selon le NIST SP 800-53 v5.2, les exigences d'un contrôle peuvent être évalués sur deux différentes portées :

- Transverse; le contrôle est appliqué de manière centralisée et uniforme à l'échelle de l'organisation. Son efficacité influence de la même manière la posture de sécurité de tous les secteurs et départements.
- Système par système; le contrôle est applicable sur certains systèmes, infrastructures ou applications et est non applicable sur d'autres.

La définition de la portée influence l'interprétation des résultats.

Niveau de confiance attendu

Le niveau de confiance fait référence à la robustesse des intrants utilisés pour obtenir le résultat de l'évaluation. L'équipe centrale défini le niveau de confiance attendu pour chaque évaluation. Un exemple d'échelle de niveau de confiance est disponible à l'Annexe 5. Pour résumer simplement le principe, un jugement d'expert permet d'obtenir un résultat d'évaluation rapidement, mais avec un faible niveau de confiance. À l'inverse, un test de sécurité offensive, qui évalue la réactivité d'un contrôle lors d'une attaque, fournit un niveau de confiance beaucoup plus élevé. Plus le niveau de confiance est élevé, plus la crédibilité du résultat augmente.

Ce concept est particulièrement important à considérer lors du développement du plan d'évaluation, car un niveau de confiance élevé permet à votre organisation d'utiliser les résultats d'Imperium comme intrant lors d'audit et de visite d'un régulateur. En contrepartie un niveau de confiance élevé engendre des coûts supérieurs et du temps supplémentaire, considérant les intrants requis pour compléter l'évaluation (généralement une collecte d'évidence et des revues des résultats par une tierce partie). Une technique intéressante consiste à définir un niveau de confiance différent selon les contrôles. Par exemple, les contrôles liés à

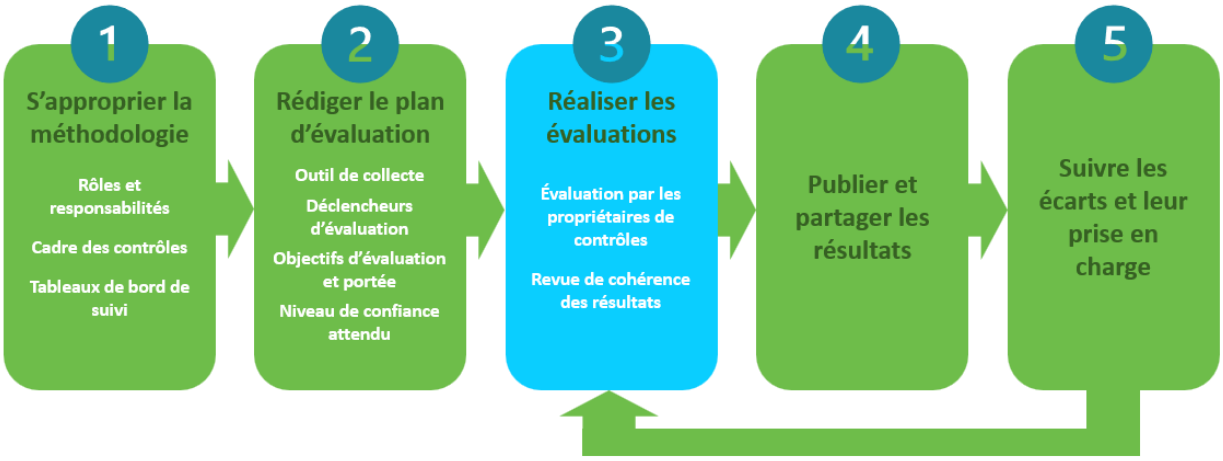
une obligation réglementaire auront un niveau de confiance attendu plus élevé afin de réutiliser les résultats.

Expérience d'entreprises ayant implémenter Imperium

Malgré le niveau de confiance plus faible, il est fortement recommandé de débuter le premier cycle d'évaluation en utilisant le jugement d'expert comme intrant. Cette approche permet d'obtenir une posture de sécurité globale en limitant les coûts et ainsi démontrer rapidement aux exécutifs l'utilité d'investir dans ce programme. Le jugement d'expert rehausse aussi l'imputabilité des parties visés.

Il est également primordial de prendre un moment pour analyser la documentation qui existe déjà dans l'organisation et qui pourrait alimenter les évaluations. Par exemple, des rapports d'audit ayant été réalisés dans les deux dernières années sont un excellent point de départ pour avoir une première posture.

3. Réaliser l'évaluation des contrôles



L'évaluation des contrôles correspond à la collecte des jugements d'experts et des preuves permettant de confirmer si un contrôle est satisfaisant. Les résultats

pourront par la suivre être agrégés pour mesurer l'efficacité de ces contrôles ainsi que la posture de sécurité de l'information de l'organisation.

La terminologie qui sera utilisée dans le chapitre est importante pour bien comprendre les nuances entre les différents concepts et résultats impliqués dans la réalisation des évaluations. À titre de rappel ou de précision, voici les termes à retenir :

- **Contrôle** : Tel que discuté précédemment, un contrôle peut prendre différentes formes : il peut être un processus, un outil technologique, un système ou même un humain. Ce sont les exigences du contrôle qui sont évaluées pour confirmer la satisfaction du contrôle.
- **Exigence** : Un contrôle est composé d'un nombre variable d'exigences. Ces exigences constituent les objectifs d'évaluation permettant de confirmer globalement si le contrôle est satisfaisant. Chaque exigence est évaluée individuellement par le propriétaire du contrôle.
- **Satisfaction** : Le résultat de l'évaluation est illustré par trois choix de réponse : 1) Satisfaisant, 2) Non satisfaisant et 3) Non applicable.
- **Efficacité** : L'efficacité est présentée en pourcentage. Elle représente la proportion d'exigences du contrôle qui est satisfaisante sur le nombre total d'exigences du contrôle.
- **Portée** : Aussi nommée couverture, la portée réfère au fait qu'un contrôle est appliqué partout où il devrait l'être. La portée est présentée sous forme de pourcentage indiquant le niveau de déploiement du contrôle par rapport à sa portée cible (par exemple : 5 applications sur 10 donc 50% de couverture).
- **Niveau de confiance** : Le niveau de confiance fait référence à la robustesse des intrants utilisés pour réaliser l'évaluation. L'équipe centrale définit le niveau de confiance attendu pour chaque évaluation.

Évaluation par les propriétaires de contrôles

La réalisation des évaluations est principalement portée par l'équipe centrale et les propriétaires de contrôles. L'équipe centrale a la responsabilité de lancer les demandes d'évaluations, au besoin, en faisant appel aux rôles de soutien discutés dans la section *Rôles et responsabilités* (page 10). Une fois les demandes lancées, les propriétaires de contrôle utiliseront l'outil de collecte sélectionné par l'équipe centrale pour saisir les résultats suivants :

- Le résultat d'évaluation pour chaque exigence associée à un contrôle. Les options sont :
    - Satisfaisante : L'exigence est atteinte sur la portée évaluée et produit un résultat entièrement acceptable.
    - Autre que satisfaisante : Des anomalies potentielles impactent l'atteinte de l'exigence sur la portée évaluée. Ces anomalies devront être traitées.
    - Non applicable : L'exigence est jugée non pertinente pour le contrôle évalué.
- Le commentaire qualitatif supportant un résultat. Le commentaire est systématiquement obligatoire lorsque le résultat n'est pas « Satisfaisant ».
- Selon le niveau de confiance exigé par l'équipe centrale, le propriétaire du contrôle devra joindre à son évaluation la documentation et les preuves nécessaires pour confirmer objectivement le résultat.

L'imputabilité du résultat de l'évaluation repose sur le propriétaire de contrôle. Cependant, il est possible d'éliminer l'étape de saisie manuelle dans l'outil de collecte en automatisant la collecte des évidences. Dans ce contexte, il incombera au propriétaire du contrôle de confirmer son adhésion à l'information collectée. Une collecte automatisée peut être alimentée par les outils de surveillance existants et

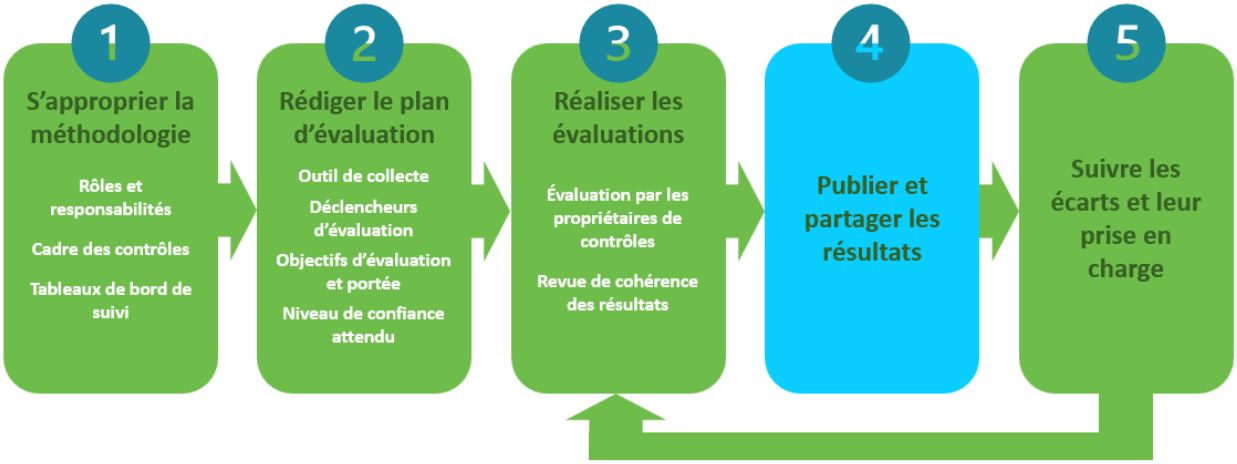
des tests continues déjà en place tel que des scans de conformités ou de vulnérabilités.

Revue de cohérence des résultats

Afin de compléter l'évaluation, une revue de cohérence est effectuée dans le but de confirmer que les informations utilisées et les constats obtenus sont complets et cohérents. À ces fins, l'équipe centrale vérifie la qualité des commentaires qualitatifs et des pièces justificatives reçues et leur pertinence avec les exigences qu'ils supportent. Au besoin, ils retournent vers le propriétaire de contrôle pour des précisions. Cette revue est essentielle afin de s'assurer que les résultats puissent être utilisés de manière fiable pour orienter les décisions et ainsi être publiés dans les tableaux de bord Imperium.

Dans une optique de rehaussement le niveau de confiance des résultats, une seconde revue de cohérence peut être réalisée par une équipe distincte (ex. : 2e ligne de défense d'une organisation). Cette technique augmente l'indépendance de la revue et confirme que les résultats sont compréhensibles et pourraient être réutilisés, par exemple pour répondre à un audit. Plus la revue est structurée et indépendante, plus l'organisation peut s'appuyer sur le résultat.

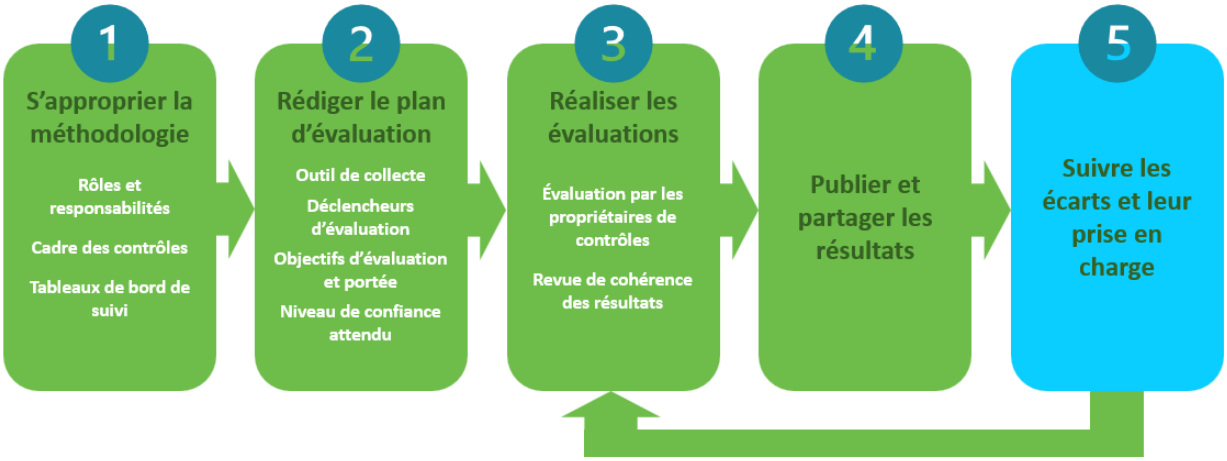
4. Publier et partager les résultats



La publication des résultats transforme l'ensemble des informations recueillies dans l'outil de collecte en un tableau de bord structuré et adapté aux différents publics. Le tableau de bord ainsi que tous les détails des indicateurs à y inclure sont présentés dans la section *Tableaux de bord de suivi* (page 22).

Une fois que les résultats d'évaluation sont intégrés dans le tableau de bord de suivi, l'équipe centrale partage le contenu avec les publics cibles. Si des résultats sont obtenus de façon automatisée, il est recommandé de mettre à jour les résultats quotidiennement afin d'offrir une posture à jour.

5. Suivre les écarts et leur prise en charge



La finalité du programme Imperium est d'améliorer la posture de sécurité de l'information de l'organisation en identifiant les zones de rehaussement par l'identification des contrôles partiellement efficaces ou inefficaces. Pour ce faire, votre organisation doit mettre en place un mécanisme de suivi des écarts.

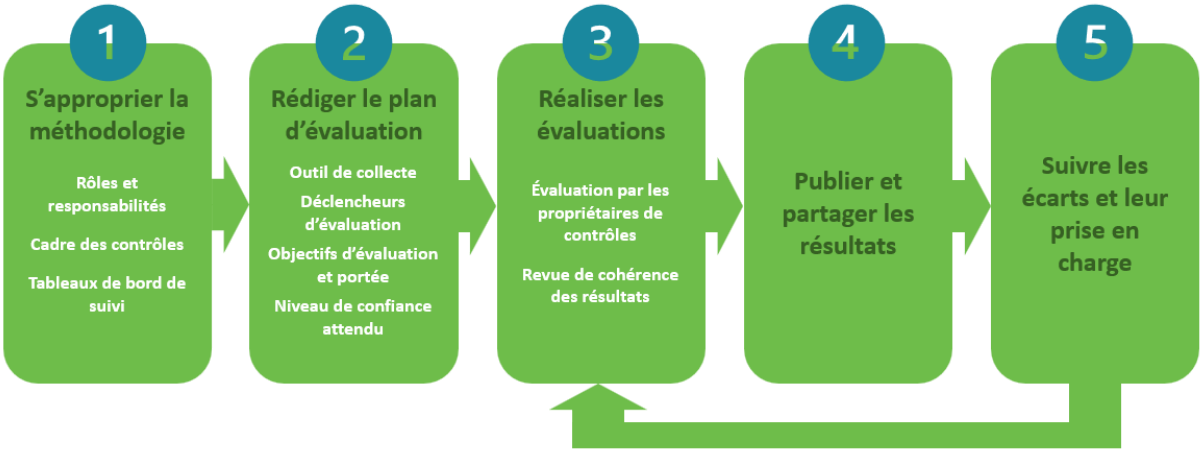
Le mécanisme de suivi des écarts doit inclure une échelle de criticité des écarts, un délai prescrit pour corriger les écarts en fonction de leur criticité et un processus de suivi de la prise en charge de ces écarts qui inclut l'outil retenu pour documenter le plan d'action, l'échéancier et le dépôt des évidences suivant la complétion du plan d'action. Idéalement, l'outil de suivi des écarts est le même que l'outil de collecte. Il faudra ainsi inclure les champs requis dans cet outil.

L'échelle de criticité des écarts définit la priorisation de la prise en charge de ceux-ci afin d'orienter les efforts là où l'impact sur la posture de sécurité est le plus significatif. Par exemple, il est recommandé que les écarts liés à un contrôle vital soient considérés les plus critiques. Votre organisation doit définir son niveau de tolérance face aux écarts et définir le mécanisme de suivi en conséquence. Il est possible de ne pas suivre tous les écarts. Un exemple serait :

Niveau de priorisation du contrôle ayant un écart	Criticité de l'écart	Délai prescrit
Vital	Très élevé	90 jours
De base	Élevé	180 jours
Lié à la zone de risque	Modéré	365 jours
Lié aux stratégies	Faible	*Aucun suivi*

Le propriétaire de contrôle est avisé de l'écart et peut définir le plan d'action approprié pour corriger la situation. Il est responsable de définir les actions à prendre et d'identifier les responsables de ces actions. Le suivi de la prise en charge est réalisé par l'équipe centrale qui peut être accompagné, au besoin, par les rôles de soutien présentés dans la section *Rôles et responsabilités* (page 10).

Une fois les correctifs en place, l'évaluation du contrôle doit être révisée. Ce qui signifie un retour à l'étape 3 du processus.



Conclusion

Le programme Imperium offre aux organisations une approche structurée, mesurable et durable permettant de renforcer leur gouvernance de la sécurité de l'information. En combinant un cadre normatif robuste, une méthodologie claire, des mécanismes d'évaluation rigoureux et un suivi transparent, Imperium permet d'obtenir une lecture continue et fiable de l'efficacité des contrôles de sécurité.

En adoptant Imperium, les organisations se dotent d'un dispositif capable de soutenir la prise de décision, d'orienter les investissements, de prioriser les efforts de remédiation et de répondre efficacement aux attentes croissantes des régulateurs et des parties prenantes internes. L'approche modulaire et progressive du programme permet également de démarrer simplement, puis d'augmenter graduellement le niveau d'automatisation, la maturité des évaluations et la robustesse de la gouvernance.

Au-delà des outils et des processus, Imperium repose sur la collaboration, la transparence et l'imputabilité partagée. En engageant les équipes, en clarifiant les rôles et en favorisant une compréhension commune des risques et des priorités, le programme contribue à créer une culture où la sécurité de l'information devient un réflexe organisationnel.

En somme, Imperium constitue un levier stratégique pour améliorer la posture de sécurité de manière tangible et durable, réduire les risques, optimiser l'allocation des ressources et positionner les organisations parmi les leaders en gouvernance de la sécurité de l'information.

Liste des annexes

Annexe 1 | Liste des domaines de sécurité de l'information

Annexe 2 | Arbre décisionnel Imperium (identification et priorisation des contrôles)

Annexe 3 | Liste des contrôles vitaux

Annexe 4 | Liste des scénarios de risques de sécurité de l'information et contrôles associés

Annexe 5 | Exemple d'échelle de niveau de confiance

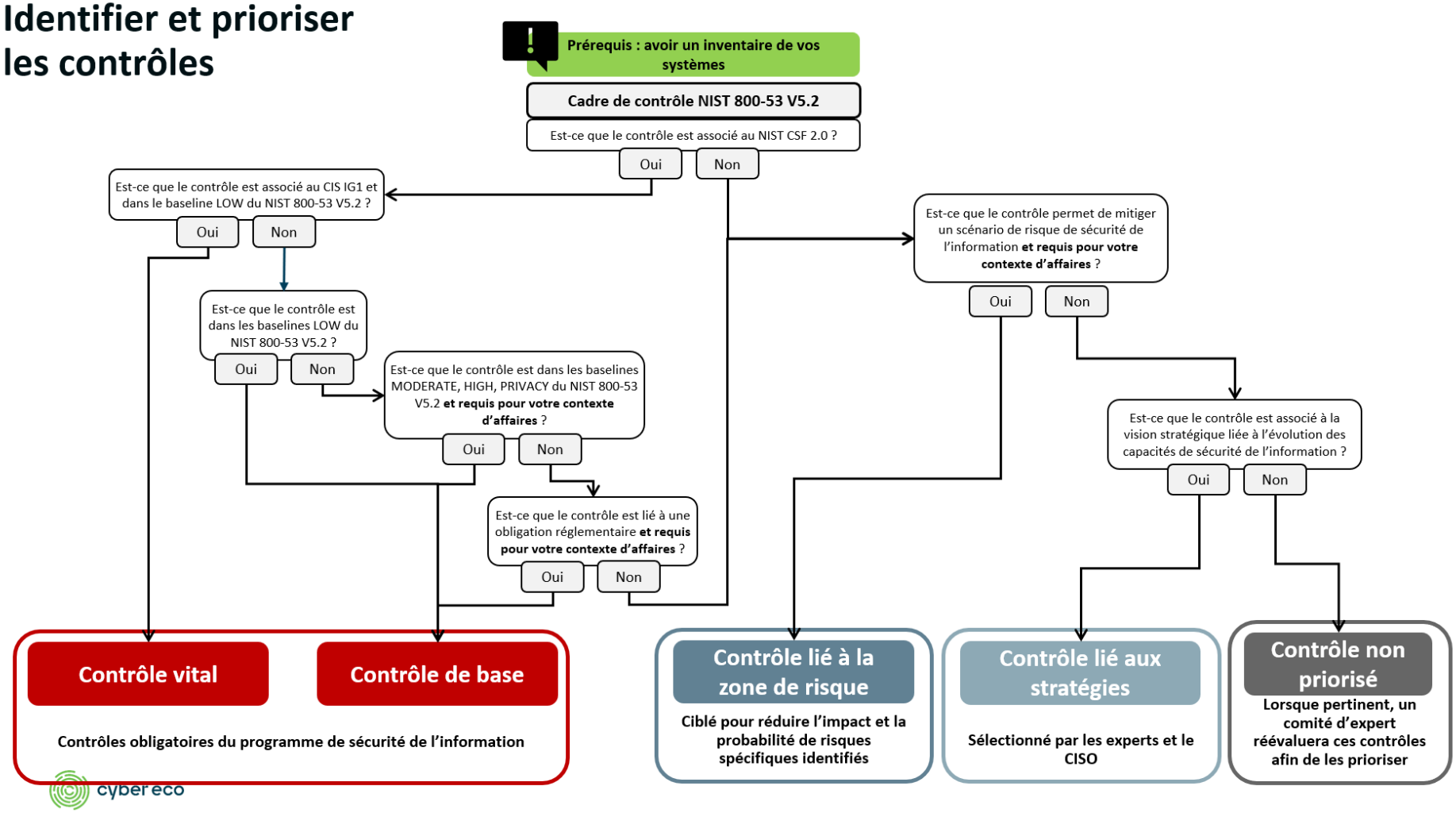
Annexe 1 | Liste des domaines de sécurité de l'information

Cette annexe présente deux exemples de listes de domaines de sécurité de l'information pouvant être utilisées pour découper votre cadre de contrôles.

Liste de domaines inspirés du NIST CSF 2.0	Liste de domaine inspirés d'un entreprise membre de CyberEco
Gouverner : • Cadre de gestion du risque de sécurité de l'information • Contexte légal, réglementaire et de l'industrie • Encadrements • Gestion de la sécurité des tiers • Gestion du programme de sécurité de l'information • Rôles et responsabilités Identifier : • Gestion de l'évaluation des risques, menaces et vulnérabilités • Gestion des actifs • Gestion des améliorations continues en SI Détecter • Investigation des événements détectés • Surveillance continue Protéger • Gestion de la résilience des technologies • Gestion de la sensibilisation et de la formation • Gestion des identités et des accès • Protection des données et cryptographie • Sécurité liée aux infrastructures et aux développements	• Cryptographie • Détection et Réponse • Gestion des identités et des accès • Gestion des vulnérabilités • Gouvernance, Risque et Conformité • Sécurité de l'infrastructure • Sécurité des données • Sécurité des tiers • Sécurité du code et des applications • Sécurité offensive • Surveillance des configurations

Remédier • Communication et coordination de la reprise • Exécution de la reprise Répondre • Communication et rendre compte des incidents de sécurité • Confinement et éradication des incidents de sécurité • Forensique des incidents de sécurité • Réponse aux incidents de sécurité	

Annexe 2 | Arbre décisionnel Imperium (identification et priorisation des contrôles)



Annexe 3 | Liste des contrôles vitaux

Famille	ID Contrôle	Nom du contrôle
Access Control	AC-1	Policy and Procedures
Access Control	AC-2	Account Management
Access Control	AC-18	Wireless Access
Access Control	AC-19	Access Control for Mobile Devices
Access Control	AC-3	Access Enforcement
Awareness and Training	AT-1	Policy and Procedures
Awareness and Training	AT-2	Literacy Training and Awareness
Audit and Accountability	AU-1	Policy and Procedures
Audit and Accountability	AU-2	Event Logging
Audit and Accountability	AU-11	Audit Record Retention
Audit and Accountability	AU-12	Audit Record Generation
Assessment, Authorization, and Monitoring	CA-9	Internal System Connections
Configuration Management	CM-1	Policy and Procedures
Configuration Management	CM-6	Configuration Settings
Configuration Management	CM-7	Least Functionality
Configuration Management	CM-8	System Component Inventory
Configuration Management	CM-10	Software Usage Restrictions
Configuration Management	CM-11	User-installed Software
Contingency Planning	CP-2	Contingency Plan
Contingency Planning	CP-9	System Backup
Contingency Planning	CP-10	System Recovery and Reconstitution
Configuration Management	CM-2	Baseline Configuration
Identification and Authentication	IA-4	Identifier Management
Identification and Authentication	IA-5	Authenticator Management
Incident Response	IR-1	Policy and Procedures
Incident Response	IR-5	Incident Monitoring
Incident Response	IR-6	Incident Reporting
Incident Response	IR-7	Incident Response Assistance
Incident Response	IR-8	Incident Response Plan
Risk Assessment	RA-2	Security Categorization
Risk Assessment	RA-5	Vulnerability Monitoring and Scanning
Risk Assessment	RA-7	Risk Response
System and Services Acquisition	SA-3	System Development Life Cycle
System and Services Acquisition	SA-8	Security and Privacy Engineering Principles
System and Services Acquisition	SA-22	Unsupported System Components
System and Communications Protection	SC-7	Boundary Protection

System and Information Integrity	SI-12	Information Management and Retention
System and Information Integrity	SI-2	Flaw Remediation
System and Information Integrity	SI-3	Malicious Code Protection
Supply Chain Risk Management	SR-12	Component Disposal

Annexe 4 | Liste des scénarios de risques de sécurité de l'information et contrôles associés

Scénario	Description	Groupe de contrôles
Attaque DDOS	Un acteur externe malicieux surcharge la capacité de la bande passante ou de traitement d'une ressource par l'envoi massif de requêtes résultant en une coupure ou dégradation prolongée de services.	SC-5 - SYSTEM AND COMMUNICATIONS PROTECTION : Denial-Of-Service Protection
		CP-2 - CONTINGENCY PLANNING : Contingency Plan
		CP-8 - CONTINGENCY PLANNING : Telecommunications Services
		AC-4 - ACCESS CONTROL : Information Flow Enforcement
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		AC-17 - ACCESS CONTROL : Remote Access
		SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
Communication d'information confidentielle ou plus au mauvais destinataire	Un acteur interne non-malicieux de l'organisation envoie par erreur de l'information confidentielle ou plus à des destinataires non-autorisés.	AT-2 - AWARENESS AND TRAINING : Literacy Training and Awareness
		IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		PS-6 - PERSONNEL SECURITY : Access Agreements
		AC-17 - ACCESS CONTROL : Remote Access
		MP-6 - MEDIA PROTECTION : Media Sanitization
		PS-3 - PERSONNEL SECURITY : Personnel Screening
Conservation inconnue d'information confidentielle ou plus	Un acteur interne non-malicieux accède à de l'information confidentielle ou plus conservée par une unité d'affaires sans connaissance claire de la portée et du volume d'information confidentielle ou plus présente.	AC-4 - ACCESS CONTROL : Information Flow Enforcement
		AC-2 - ACCESS CONTROL : Account Management
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
		AT-2 - AWARENESS AND TRAINING : Literacy Training and Awareness
		AT-3 - AWARENESS AND TRAINING : Role-based Training
		CM-8 - CONFIGURATION MANAGEMENT : System Component Inventory
Contournement des mécanismes de sécurité	Un acteur interne malicieux contourne les mécanismes de sécurité en place et accède à de l'information confidentielle ou plus.	AC-3 - ACCESS CONTROL : Access Enforcement
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		AC-4 - ACCESS CONTROL : Information Flow Enforcement
		AC-2 - ACCESS CONTROL : Account Management
		SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring

		CA-3 - ASSESSMENT, AUTHORIZATION, AND MONITORING : Information Exchange
Enregistrement externe sur un emplacement non adéquat	Un tiers non-malicieux consulte et copie sur un support non géré (ex: clé USB, cloud privé) des correspondances ou rapports contenant de l'information confidentielle ou plus.	SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
		AU-2 - AUDIT AND ACCOUNTABILITY : Event Logging
		AT-2 - AWARENESS AND TRAINING : Literacy Training and Awareness
		IR-9 - INCIDENT RESPONSE : Information Spillage Response
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		AC-20 - ACCESS CONTROL : Use of External Systems
Enregistrement interne sur un emplacement non adéquat	Un acteur interne non-malicieux consulte et copie sur un support non géré par l'organisation (ex: clé USB, cloud privé) des correspondances ou rapports contenant de l'information confidentielle ou plus.	AC-6 - ACCESS CONTROL : Least Privilege
		SC-28 - SYSTEM AND COMMUNICATIONS PROTECTION : Protection of Information at Rest
		AT-2 - AWARENESS AND TRAINING : Literacy Training and Awareness
		AU-2 - AUDIT AND ACCOUNTABILITY : Event Logging
		SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
		CM-8 - CONFIGURATION MANAGEMENT : System Component Inventory
		PS-6 - PERSONNEL SECURITY : Access Agreements
Exploitation de la gestion d'accès	Un acteur interne malicieux exploite des manquements dans la gestion d'accès et autorisations (exemple : principe du moindre privilège, enregistrement sur emplacement non adéquat...) et accède de manière autorisée à de l'information confidentielle ou plus.	AC-4 - ACCESS CONTROL : Information Flow Enforcement
		AU-2 - AUDIT AND ACCOUNTABILITY : Event Logging
		IA-2 - IDENTIFICATION AND AUTHENTICATION : Identification and Authentication (Organizational Users)
		IA-12 - IDENTIFICATION AND AUTHENTICATION : Identity Proofing
		AC-2 - ACCESS CONTROL : Account Management
		AC-3 - ACCESS CONTROL : Access Enforcement
Exploitation de vulnérabilité d'une solution interne	Un acteur externe malicieux exploite une vulnérabilité / faille de sécurité (Ex : protocole d'authentification inadapté...) connue, mais non-corrigée dans une solution interne et accède à de l'information confidentielle ou plus.	SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
		IR-4 - INCIDENT RESPONSE : Incident Handling
		SA-3 - SYSTEM AND SERVICES ACQUISITION : System Development Life Cycle
		RA-5 - RISK ASSESSMENT : Vulnerability Monitoring and Scanning
		SI-2 - SYSTEM AND INFORMATION INTEGRITY : Flaw Remediation
Exploitation de zero day	Un acteur externe malicieux exploite une faille de sécurité inconnue de type "zero day" dans une solution interne et accède à de l'information confidentielle ou plus.	IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
		CM-8 - CONFIGURATION MANAGEMENT : System Component Inventory

		SA-3 - SYSTEM AND SERVICES ACQUISITION : System Development Life Cycle
		SA-10 - SYSTEM AND SERVICES ACQUISITION : Developer Configuration Management
Exploitation d'erreur de configuration	Un acteur externe malicieux exploite une erreur de configuration dans une solution interne et accède à de l'information confidentielle ou plus.	IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		CM-3 - CONFIGURATION MANAGEMENT : Configuration Change Control
		RA-5 - RISK ASSESSMENT : Vulnerability Monitoring and Scanning
		MP-6 - MEDIA PROTECTION : Media Sanitization
		CM-6 - CONFIGURATION MANAGEMENT : Configuration Settings
Hameçonnage/Harponnage	Un acteur externe malicieux envoie via un canal de communication des messages piégés contenant des procédés illégitimes à un utilisateur soigneusement identifié ou un groupe d'utilisateurs qui, une fois exécutés accède à de l'information confidentielle ou plus.	IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		SI-3 - SYSTEM AND INFORMATION INTEGRITY : Malicious Code Protection
		AT-2 - AWARENESS AND TRAINING : Literacy Training and Awareness
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		AC-2 - ACCESS CONTROL : Account Management
Incident d'un tiers	Un tiers non-malicieux est victime d'un incident causant une brèche de confidentialité et/ou disponibilité et/ou intégrité de ses données (exemple : vulnérabilité dans une solution commerciale/open-source, manquement de configuration, etc) compromettant les données de l'organisation.	IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
		SA-4 - SYSTEM AND SERVICES ACQUISITION : Acquisition Process
		SR-6 - SUPPLY CHAIN RISK MANAGEMENT : Supplier Assessments and Reviews
		SA-9 - SYSTEM AND SERVICES ACQUISITION : External System Services
Interception de données	Un acteur interne malicieux intercepte volontairement de l'information confidentielle ou plus (ex : man in the middle, keylogger, écoute d'appel...).	SI-2 - SYSTEM AND INFORMATION INTEGRITY : Flaw Remediation
		RA-1 - RISK ASSESSMENT : Policy and Procedures
		IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		AC-3 - ACCESS CONTROL : Access Enforcement
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		SC-8 - SYSTEM AND COMMUNICATIONS PROTECTION : Transmission Confidentiality and Integrity

		SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
		SC-23 - SYSTEM AND COMMUNICATIONS PROTECTION : Session Authenticity
Intrus physique : contournement de contrôles logiques	Un acteur externe malicieux s'introduit dans un bureau ou dans la salle serveur et gagne accès à de l'information confidentielle ou plus en contournant les contrôles de sécurité logiques (ex : introduction d'une clé USB dans des ordinateurs pour y introduire des logiciels malveillants)	SI-7 - SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
		SI-3 - SYSTEM AND INFORMATION INTEGRITY : Malicious Code Protection
		SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
		IR-2 - INCIDENT RESPONSE : Incident Response Training
		IR-4 - INCIDENT RESPONSE : Incident Handling
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		CM-3 - CONFIGURATION MANAGEMENT : Configuration Change Control
Intrus physique : interruption de services	Un acteur externe malicieux s'introduit dans un bureau ou dans la salle serveur et pose une action visant à interrompre un service (ex : interconnecter deux prises RJ45 du LAN avec un fil d'ordinateur pour créer une panne de réseau, dissimuler des super aimants ou transmetteurs clandestins)	CP-9 - CONTINGENCY PLANNING : System Backup
		IR-2 - INCIDENT RESPONSE : Incident Response Training
		IR-4 - INCIDENT RESPONSE : Incident Handling
		PS-3 - PERSONNEL SECURITY : Personnel Screening
		PS-7 - PERSONNEL SECURITY : External Personnel Security
Intrus physique : vol de documents	Un acteur externe malicieux s'introduit dans un bureau pour voler des documents sensibles laissés sur les espaces de travail.	IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-2 - INCIDENT RESPONSE : Incident Response Training
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		PS-7 - PERSONNEL SECURITY : External Personnel Security
		PS-3 - PERSONNEL SECURITY : Personnel Screening
Rançongiciel	Un acteur externe malicieux prend en otage un actif (serveur, appareil...) et demande une rançon en échange d'une clé permettant de déchiffrer les données chiffrées.	CP-9 - CONTINGENCY PLANNING : System Backup
		IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		SI-2 - SYSTEM AND INFORMATION INTEGRITY : Flaw Remediation
		SI-3 - SYSTEM AND INFORMATION INTEGRITY : Malicious Code Protection
		AC-17 - ACCESS CONTROL : Remote Access
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		RA-5 - RISK ASSESSMENT : Vulnerability Monitoring and Scanning

Snooping par un acteur interne	Un acteur interne malicieux recherche les repértoires, applications, bases de données et dépots partagés et accède à de l'information confidentielle ou plus.	AC-3 - ACCESS CONTROL : Access Enforcement
		AC-6 - ACCESS CONTROL : Least Privilege
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		MP-6 - MEDIA PROTECTION : Media Sanitization
		SI-4 - SYSTEM AND INFORMATION INTEGRITY : System Monitoring
		IR-9 - INCIDENT RESPONSE : Information Spillage Response
		AC-2 - ACCESS CONTROL : Account Management
		SI-12 - SYSTEM AND INFORMATION INTEGRITY : Information Management and Retention
Snooping par un tiers	Un tiers malicieux recherche les repértoires, applications et dépots partagés et accède à de l'information confidentielle ou plus.	AC-2 - ACCESS CONTROL : Account Management
		AC-3 - ACCESS CONTROL : Access Enforcement
		AC-4 - ACCESS CONTROL : Information Flow Enforcement
		AC-6 - ACCESS CONTROL : Least Privilege
		IA-12 - IDENTIFICATION AND AUTHENTICATION : Identity Proofing
		IR-9 - INCIDENT RESPONSE : Information Spillage Response
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		PS-6 - PERSONNEL SECURITY : Access Agreements
		SC-28 - SYSTEM AND COMMUNICATIONS PROTECTION : Protection of Information at Rest
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		SI-12 - SYSTEM AND INFORMATION INTEGRITY : Information Management and Retention
Utilisation d'un Shadow IT (solution infonuagique)	Un acteur interne non-malicieux exfiltre de l'information confidentielle ou plus en utilisant une solution infonuagique non-approuvée ayant des accès non controlés et non sécurisés.	AC-17 - ACCESS CONTROL : Remote Access
		AC-2 - ACCESS CONTROL : Account Management
		AT-2 - AWARENESS AND TRAINING : Literacy Training and Awareness
		AU-2 - AUDIT AND ACCOUNTABILITY : Event Logging
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
		SC-8 - SYSTEM AND COMMUNICATIONS PROTECTION : Transmission Confidentiality and Integrity
Utilisation d'un Shadow IT (solution Interne)	Un acteur interne non-malicieux accède à de l'information confidentielle ou plus en utilisant une solution développée en milieu	AC-4 - ACCESS CONTROL : Information Flow Enforcement
		AT-2 - AWARENESS AND TRAINING : Literacy Training and Awareness
		AU-2 - AUDIT AND ACCOUNTABILITY : Event Logging

	utilisateur vulnérable (ex : accès non controlés et non sécurisés...).	CA-3 - ASSESSMENT, AUTHORIZATION, AND MONITORING : Information Exchange
		MP-6 - MEDIA PROTECTION : Media Sanitization
		SC-28 - SYSTEM AND COMMUNICATIONS PROTECTION : Protection of Information at Rest
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection
Vol/perte d'appareil mobile	Un acteur externe malicieux vole l'appareil mobile d'un employé ou s'empare d'un appareil mobile perdu, accède à la session et à de l'information confidentielle ou plus stockée sur l'appareil ou à travers le réseau interne de l'organisation en se connectant à une borne WiFi.	AC-17 - ACCESS CONTROL : Remote Access
		AU-2 - AUDIT AND ACCOUNTABILITY : Event Logging
		IA-2 - IDENTIFICATION AND AUTHENTICATION : Identification and Authentication (Organizational Users)
		IR-4 - INCIDENT RESPONSE : Incident Handling
		IR-8 - INCIDENT RESPONSE : Incident Response Plan
		PM-1 - PROGRAM MANAGEMENT : Information Security Program Plan
		SC-7 - SYSTEM AND COMMUNICATIONS PROTECTION : Boundary Protection

Annexe 5 | Exemple d'échelle de niveau de confiance

Niveau de confiance	Description
Non évalué	L'évaluation du contrôle n'a jamais été effectuée ou le contrôle n'est pas encore déployé.
Évaluation par jugement d'expert	L'évaluation du contrôle a été effectuée par une personne ayant certaines connaissances du contrôle à l'aide de quelques évidences à l'appui.
Auto-évaluation	L'évaluation du contrôle a été effectuée par le propriétaire du contrôle ou le responsable d'évaluation assigné par celui-ci
Auto-évaluation approuvée	L'évaluation du contrôle a été approuvée par le propriétaire du contrôle (minimum signataire Directeur/Directrice principale).
Revue objective 2LDD de l'auto-évaluation	Une revue de l'auto-évaluation a été effectuée par une équipe de deuxième ligne de défense (2LDD).
Revue 3LDD	Une revue des efficacités de contrôle a été effectuée par une équipe de troisième ligne de défense (3LDD).
Évaluation indépendante du contrôle à une date donnée	Une équipe externe a évalué le contrôle en utilisant un cadre de contrôle indépendant (ex. SOC 2 Type 1, ISO27001) ou d'autres normes/standards autoritaires officielles, couvrant la posture à une date donnée, mais ne couvrant pas l'efficacité des contrôles sur une période.
Surveillance manuelle de l'efficacité du contrôle ou vérification externe couvrant une période	• Une équipe de contrôle de la qualité effectue une surveillance manuelle et régulière de l'efficacité du contrôle (ex. pour détecter des erreurs et anomalies) avec un échantillonnage acceptable. • Une vérification externe couvrant l'efficacité des contrôles sur une période donnée, basée sur des tests de contrôle incluant l'échantillonnage représentatif de l'ensemble de la période (ex. SOC 2 Type 2 ou autres normes/standards autoritaires officielles).
Test de robustesse du contrôle	Une équipe indépendante de sécurité (ex. Purple team) a effectué un test sur la robustesse du contrôle.
Surveillance en continu de l'efficacité du contrôle	Une surveillance en continu est effectuée sur l'efficacité du contrôle (ex. pour détecter des erreurs et anomalies) à travers des outils technologiques automatisés.