GOUVERNANCE ET RISQUES

DOSSIER TECHNIQUE

LE **CONTRÔLE PERMANENT** CYBER

1 Tous publics 2 Avancé 3 Expert

Mars 2026

Contrôle permanent de niveau 2 et cybersécurité : principes, exemples et bonnes pratiques

CLUSIF

L’article L. 122-5 de la propriété intellectuelle n’autorisant pas les représentations ou reproduction intégrale, ou partielle, faite sans le consentement de l’auteur ou de l’ayant droit ou ayant cause, sauf exception stricte (« copies ou reproductions réalisées à partir d’une source licite et strictement réservées à l’usage privé du copiste et non destinées à une utilisation collective », analyses et les courtes citations dans un but d’exemple et d’illustration, etc.), toute représentation ou reproduction, par quelque procédé que ce soit du présent document sans autorisation préalable du Clusif constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Table des matières

1 ARGUMENTAIRE ET PRESENTATION DE LA METHODOLOGIE 6

2 CONTROLE INTERNE : UTILITE, FORME ET LIEN AVEC LA SECURITE DE L'INFORMATION 7

2.1 Rapide historique du contrôle interne 7

2.2 Objet du contrôle interne 8

2.3 Contrôle interne et cybersécurité 9

2.4 Focus sur le contrôle permanent de niveau 2 10

2.4.1 Comment assure-t-il ses missions ? 10

2.5 Le plan de contrôle de niveau 2 11

2.5.1 Appréciation des résultats du plan de contrôle 12

2.6 Plan de contrôle « cybersécurité » 13

2.6.1 Caractéristiques 13

2.6.2 Exemples de thématiques pouvant être abordées dans le cadre d'un plan de contrôle cyber 13

3 LISTE DES POINTS D'ATTENTION ET DES PREREQUIS 14

4 EXEMPLES DE POINTS DE CONTROLE « CYBER » 16

4.1 Gouvernance 17

4.2 Conformité légale et réglementaire 19

4.3 Gestion des identités et des accès 20

4.4 Continuité et gestion de crise 22

4.5 Gestion des actifs 25

5 RETOUR D'EXPERIENCE DES MEMBRES DU GROUPE DE TRAVAIL 29

5.1 Mise en œuvre du projet 29

5.2 Quels ont été les facteurs de réussite de la mission ? 29

5.3 Quelles dynamiques internes ont facilité le déroulement de la mission ? 29

5.4 Quelles ont été les principales difficultés rencontrées ? 29

5.5 Quelles sont les évolutions envisagées ? 30

5.6 Quels ont été les bénéfices observés ? 30

5.7 Quel conseil donneriez-vous à une organisation qui démarre la mise en œuvre d'un projet similaire ? 30

6 LES MOTS DU CONTROLE PERMANENT 31

6.1 Les acronymes 31

6.2 Les termes à ne pas confondre 31

6.3 Glossaire 34

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les animateurs du groupe de travail :

Donatien	**KOFFI**	GENERALI
Julien	**NAU**	GRANT THORNTON

Le Clusif tient à adresser ses remerciements particuliers à

Delphine	**BARON**	MACIF

Les contributeurs :

Philippe	**ARDOUIN**	EAU17
Jean-Michel	**BESNARD**	GRANT THORNTON
Tatiana	**BOYER**	GARANCE MUTUELLE
Alban	**CAOUREN**	X43C
Mohamad	**CHANFI**	GRDF
Jimmy	**CLABAULT**	BLACKFOX PARTNER
Anthony	**CROUZET**	MINISTÈRE DES ARMÉES
Patrice	**DUHEM**	ON-X
Arnaud	**IRVOAS**	SCC France
Marie-Béatrice	**KLEINKLAUS**	CAISSE DES DÉPÔTS ET CONSIGNATIONS
Abdel-Hakim	**MAHIR**	ALLIANZ IARD
Loïc	**MENGUY**	CAISSE CENTRALE DE REASSURANCE
Hervé	**SCHAUER**	HS2
Clément	**VALOT**	BLACKFOX PARTNER
Michael	**WILECZEK**	HBD CONSULTING

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Argumentaire et présentation de la méthodologie

Le groupe de travail du Clusif « Contrôle interne cyber » s'est donné pour mission d'élaborer un guide pratique visant à intégrer la cybersécurité[1] dans les dispositifs de contrôle interne. Dans un contexte où les organisations dépendent fortement de leurs systèmes d'information, l'enjeu est de construire un cadre partagé qui articule bonnes pratiques de sécurité, référentiels de contrôle interne et gestion des risques numériques.

Le guide poursuit plusieurs objectifs : accompagner les équipes du contrôle permanent et les Responsables Sécurité des Systèmes d'information (RSSI) en témoignant de l'importance de leur rôle dans le dispositif de contrôle interne, en leur fournissant des exemples concrets de contrôles de cybersécurité adaptables à leur contexte, et enfin en proposant un cadre accessible et opérationnel permettant de renforcer la résilience de leur système face aux menaces de cybersécurité. Le guide se veut un rappel de la place centrale que la cybersécurité occupe dorénavant dans les processus métiers.

Pour répondre à ces objectifs, le groupe de travail a adopté une démarche structurée et progressive. Il a identifié un ensemble de prérequis et de questions stratégiques à se poser avant de se lancer dans un plan de contrôle permanent de cybersécurité, permettant aux organisations de situer leur maturité et leurs priorités.

Le guide propose par ailleurs des exemples concrets de contrôles de cybersécurité, illustrant la manière de relier exigences de sécurité, conformité et suivi des risques. Des retours d'expérience des membres du groupe de travail sont présentés pour aider toute organisation, quel que soit son secteur ou sa taille, à initier et structurer sa démarche. Enfin, le groupe propose des définitions de termes et concepts clés, pour créer un langage commun entre RSSI, contrôle permanent et instances de gouvernance.

Ce travail collectif se veut ainsi un outil pragmatique et opérationnel, destiné à renforcer la gouvernance et la résilience numérique des organisations.

[1] Le groupe de travail attire l'attention du lecteur sur la différence nécessaire à faire entre les termes « cybersécurité » et « sécurité du système d'information ». Le dernier chapitre du présent document présente les distinctions entre les deux termes.

2 Contrôle interne : utilité, forme et lien avec la sécurité de l'information

2.1 Rapide historique du contrôle interne

Le mécanisme de contrôle interne plonge ses racines dans l'Antiquité. Il visait alors à la bonne gestion des ressources et des trésors.

Par exemple, en Égypte ancienne, pour la gestion des stocks de céréales, les scribes enregistraient les quantités entrantes et sortantes, ce qui correspond à une forme de traçabilité. On recourait également au « contrôle à quatre yeux » pour limiter les risques de fraude.

Dans la Rome antique, les dépenses publiques ne pouvaient être engagées qu'après autorisation écrite et signature d'un magistrat, ce qui correspond à une procédure d'autorisation formelle.

La forme contemporaine du contrôle interne, auquel ce document fait référence, s'est imposée à partir du XX^{e} siècle, à la suite du krach boursier de 1929 aux États-Unis et de la révélation du manque de fiabilité des informations financières.

De plus en plus d'entreprises le mettent en œuvre aujourd'hui[2] pour répondre à des besoins de sécurité, de transparence, de qualité, de satisfaction client, ou encore de conformité.

[2] Pour permettre de clarifier les termes utilisés dans ce document, ainsi que pour lever des sources de confusion fréquentes, ce document présente un chapitre de définitions : « Les mots du contrôle permanent ».

2.2 Objet du contrôle interne

Le contrôle interne est un dispositif global et continu de vérification. Il est mis en place pour garantir :

- la disponibilité, la confidentialité et la fiabilité du système d'information ;
- la conformité aux normes de l'entreprise (c'est-à-dire aux politiques et procédures internes), aux lois et réglementations ;
- l'efficacité des opérations / des activités de l'entreprise.

Il se découpe en deux typologies de contrôles (permanent et périodique) réalisés par trois niveaux de défense, comme le résume le schéma suivant :

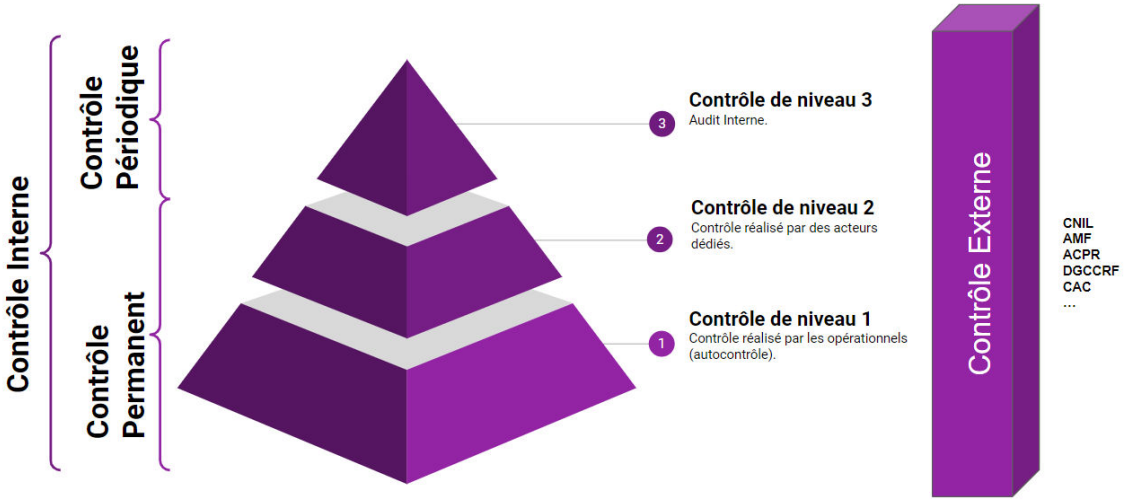


Figure 1 – Illustration du contrôle interne

Le contrôle de premier niveau est réalisé par les services opérationnels pour s'assurer de la régularité des activités.

Le contrôle de deuxième niveau, lui, est assuré par des fonctions dédiées et indépendantes des opérationnels, comme la gestion des risques, la conformité ou le contrôle financier. Il vérifie la pertinence et l'efficacité des contrôles de premier niveau. Il assure ainsi la conformité, la sécurité des opérations, la bonne application des politiques internes et la gestion cohérente des risques à l'échelle de l'entreprise.

Enfin, le contrôle de troisième niveau est à la charge de l'audit interne. Il offre notamment une vue objective sur la conformité aux exigences réglementaires et l'efficacité de la gestion des opérations, incluant la gestion des risques et des contrôles. Pour que le dispositif de contrôle interne soit efficient, le contrôle de niveau 3 doit être assuré par une fonction totalement indépendante des fonctions de contrôle de permanent de niveau 1 et 2.

L'efficacité du dispositif de contrôle interne repose sur l'alignement stratégique et la cohérence opérationnelle de ses trois lignes de défense. Seule une démarche harmonisée et coordonnée, s'appuyant sur un référentiel commun de contrôles, peut garantir la continuité et la cohérence des messages adressés aux directions métiers. Cet alignement est par ailleurs indispensable pour éviter la duplication des efforts, les contradictions dans les analyses et, in fine, pour fournir une assurance objective et un pilotage efficace.

Afin de concrétiser cet alignement et d'assurer une gestion intégrée des objectifs, il peut être pertinent de mettre en place une instance de pilotage, dont la mission essentielle sera de garantir la cohérence et l'articulation du plan de contrôle global intégrant les activités des trois niveaux de défense

2.3 Contrôle interne et cybersécurité

Le contrôle interne a initialement été imposé pour protéger les actifs financiers de l'entreprise et garantir la fiabilité des informations financières par des lois, telles que :

- la loi Bâle (Bâle I en 1988, Bâle II en 2004, Bâle III en 2010-2017, Bâle IV en 2022-2025) ;
- la loi Sarbanes-Oxley (SOX) de 2002 aux États-Unis ;
- la loi de Sécurité financière (LSF) en France en 2003 ;
- la directive européenne Solvabilité (Solvabilité I dans les années 1970, Solvabilité II dans les années 2010) ;
- la lutte contre le blanchiment de capitaux et le financement du terrorisme ;
- la loi Sapin II de 2016 ;
- etc.

Avec la digitalisation des processus et la numérisation des activités, le contrôle interne s'étend désormais à la protection de l'ensemble des actifs essentiels que sont les données et les systèmes informatiques, et non plus seulement à celle des actifs financiers. De fait, la cybersécurité fait partie intégrante du dispositif global de contrôle interne. Son rôle est d'assurer que des mesures appropriées sont en place pour :

- protéger les actifs numériques (données, systèmes informatiques, propriété intellectuelle, etc.) face aux risques d'indisponibilité, de perte d'intégrité et de confidentialité ;
- assurer l'efficacité et l'efficience des processus et des outils de protection des actifs ;
- assurer la conformité : respecter les réglementations en vigueur propres au système d'information (RGPD, DORA, NIS…) et les autres normes du secteur.

Pour atteindre ces buts, le contrôle interne « cyber » identifie et évalue les risques (impacts et probabilités) et propose des mesures d'atténuation appropriées (telles que la formalisation de politiques, de processus, de procédures ou la mise en place d'outils ou de mécanismes de supervision). L'émergence du télétravail, de la digitalisation et la multiplication des cybermenaces rendent indispensable son intégration au dispositif global de contrôle interne. Cette nécessité est renforcée par l'apparition des nouvelles réglementations (DORA, NIS 2), conjuguée aux attentes accrues des clients en matière de transparence et de sécurité de leurs données numériques. Ainsi, disposer d'un contrôle interne en cybersécurité devient stratégique pour toute entreprise souhaitant renforcer sa gestion des risques, sa réputation et sa crédibilité.

Les mesures de sécurité pouvant être perçues comme un frein à l'activité, il arrive qu'elles ne soient pas appliquées ou contournées par les responsables « métier » : le contrôle permet alors de corriger une partie de ces déviances.

En effectuant des vérifications régulières et systématiques, ce contrôle permet d'éviter le « semblant de sécurité », c'est-à-dire l'illusion que les mesures de protection mises en place sont suffisantes alors qu'aucune garantie n'est donnée sur leur correcte implémentation. L'assurance que les mesures de sécurité sont non seulement présentes, mais également efficaces renforce ainsi la confiance que peut avoir l'entreprise dans la robustesse de sa sécurité.

De plus, le contrôle interne est une manière de détecter les failles et les défauts dans les processus de sécurité avant qu'ils ne soient identifiés par des auditeurs externes, ce qui a deux vertus : tout d'abord, celle de concentrer les audits externes sur des problématiques de cybersécurité plus profondes et stratégiques (améliorant ainsi la sécurité de l'entreprise) ; ensuite, celle d'induire une réduction des coûts, en minimisant les interruptions opérationnelles d'une part et en diminuant le nombre d'audits externes nécessaires d'autre part.

Plus qu'une simple vérification, les échanges réguliers et constructifs avec les acteurs du contrôle interne constituent un vecteur essentiel de sensibilisation et d'acculturation des directions métiers, renforçant ainsi la prise de conscience et l'appropriation collective d'une culture de la maîtrise des risques au quotidien.

2.4 Focus sur le contrôle permanent de niveau 2

Parmi les différents niveaux de contrôle interne, on trouve le contrôle permanent de niveau 2, que ce guide se propose d'approfondir. Il s'agit d'un niveau particulièrement stratégique, car il agit comme un superviseur par rapport au contrôle de premier niveau, tout en étant en interaction avec le contrôle périodique (l'audit interne).

Attention : son rôle n'est pas de faire (ou de refaire) le travail du niveau 1, mais de s'assurer qu'il est bien fait, c'est-à-dire que les processus et les contrôles opérationnels sont formalisés, pertinents, efficaces et réalisés.

Pour illustrer ce positionnement :

Le contrôle de niveau 1 est dans l'action. Ce sont les joueurs sur le terrain qui marquent les buts et défendent.

Le contrôle de niveau 2 est dans l'analyse. C'est l'entraîneur adjoint ou le responsable de la performance. Son rôle est de s'assurer que les joueurs utilisent la bonne stratégie et les bonnes techniques d'entraînement, et que leurs efforts sont documentés et efficaces.

Son mandat est donc d'assurer l'ingénierie qualité du dispositif de contrôle. Il se concentre sur :

- la documentation et la compréhension par tous des processus et des procédures de contrôles opérationnels (la formalisation) ;
- la conception des contrôles pour couvrir les risques majeurs de l'activité (la pertinence) ;
- le test par échantillonnage ponctuel et indépendant des contrôles de niveau 1, en utilisant la documentation des opérationnels de la première ligne pour s'assurer qu'ils sont réalisables et qu'ils atteignent effectivement leur objectif de maîtrise des risques (l'efficacité).

Contrairement au niveau 1, qui est concentré sur son propre domaine d'expertise, le niveau 2 a une vue transversale sur l'ensemble de l'organisation. Cela lui permet d'identifier des incohérences, des anomalies, des faiblesses ou des dérives qui pourraient passer inaperçues au niveau opérationnel avant qu'elles ne deviennent des incidents majeurs. Il a un rôle important dans l'amélioration continue et le renforcement des dispositifs de contrôle. Il est aussi chargé de remonter les alertes et les informations cruciales sur les risques significatifs aux personnes qui sont en mesure d'engager juridiquement l'organisation (dirigeants, conseil d'administration, direction générale, comex…). Il aide à anticiper les crises et à préparer les plans d'action nécessaires.

2.4.1 Comment assure-t-il ses missions ?

Les missions du contrôle permanent de niveau 2 s'articulent généralement autour de :

- contrôles récurrents qui ont pour but l'appréciation de la pertinence et de l'efficacité du dispositif de contrôle et la réduction des risques du premier niveau (réalité du contrôle, exhaustivité du périmètre couvert, qualité des contrôles, pertinence de la répartition des tâches, etc.) ;
- contrôles spécifiques / thématiques, contrôles réalisés en fonction des évènements (mise en place d'une nouvelle activité, changement d'outil ou d'organisation, incidents significatifs survenus, etc.).

Les contrôles de deuxième niveau peuvent prendre différentes formes :

- contrôles documentaires dans le but de vérifier la conformité et la complétude des documents ;
- contrôles de cohérence et de vérification des calculs et des traitements ;
- contrôles de suivi d'anomalies, d'incidents, de plans d'action, etc., pour vérifier qu'ils sont bien traités et résolus ;

- contrôles de second regard pour fournir une validation indépendante sur les décisions sensibles.

Cela peut se faire avec des outils tels que :

- des contrôles sur place et/ou sur pièces ;
- des questionnaires / sondages d'auto-évaluation adressés aux opérationnels assurant le premier niveau ;
- des requêtes dans les systèmes d'information ;
- des échantillonnages.

La priorité du contrôle permanent de niveau 2 se porte sur l'efficience des contrôles « clés » visant la maîtrise des risques significatifs.

La profondeur et la périodicité des contrôles de deuxième niveau sont proportionnées à la criticité des risques. Ils sont définis sur la base de la cartographie des risques, des indicateurs d'alerte et des incidents. Lorsque le niveau de risque est jugé faible ou acceptable, le contrôle peut se limiter à l'autocontrôle de l'opérationnel, sans nécessiter de contrôle de deuxième niveau.

Les critères d'évaluation utilisés pour les contrôles de deuxième niveau doivent être révisés régulièrement afin d'inscrire le contrôle permanent de niveau 2 dans une démarche d'amélioration continue.

Attention : tout comme le contrôle de niveau 1, le contrôle de niveau 2 doit impérativement formaliser ses processus et procédures de contrôle (incluant leur fréquence, leur portée et leur méthodologie) et conserver la traçabilité exhaustive de l'exécution de chaque contrôle réalisé, ainsi que des résultats / conclusions obtenus et des plans d'action associés, pour garantir une revue probante auprès du contrôle de niveau 3 (audit interne) ou des contrôleurs externes.

2.5 Le plan de contrôle de niveau 2

Un plan de contrôle est un document essentiel dans le cadre du contrôle interne d'une organisation. C'est la feuille de route du contrôle permanent de niveau 2 qui détaille et formalise les contrôles clés à réaliser sur les processus de l'entreprise, afin de garantir la maîtrise des risques et la fiabilité des informations (financières, opérationnelles, réglementaires). Il traduit la stratégie de gestion des risques en un ensemble d'actions concrètes, documentées et suivies. Il permet de répondre aux questions :

- Quel est l'objet du contrôle (les opérations, les processus, les transactions) ?
- Qui est responsable du contrôle (la gestion des risques, le contrôle de gestion, la conformité, l'équipe RSSI, l'équipe DPO…) ?
- Quelle est la fréquence du contrôle (mensuellement, trimestriellement, semestriellement, annuellement…) ?
- Quelle est la procédure de contrôle ? Quelle est la méthode utilisée pour procéder au contrôle ?
- Quelle est la preuve de l'exécution attendue ?

Un plan de contrôle correspond donc à l'ensemble des contrôles réalisés selon une fréquence conforme à la priorisation des risques identifiés. Chaque contrôle cible un thème, un sous-thème ou un risque spécifique. Cette organisation garantit d'obtenir, à la fin de chaque campagne de contrôle, une vue complète et exhaustive des risques et des contrôles associés.

Ce document structurant est, en général, établi, validé et piloté par l'instance de gouvernance ou de pilotage du Contrôle interne mentionnée précédemment (§ 2.1)

2.5.1 Appréciation des résultats du plan de contrôle

Chaque point de contrôle est généralement évalué selon une échelle propre à chaque organisation.

Exemple d'échelle à quatre niveaux :

- **Satisfaisant** : toutes les preuves attendues sont disponibles pour répondre au point de contrôle.
- **Acceptable** : les principales preuves attendues sont disponibles pour répondre au point de contrôle.
- **À améliorer** : les principales preuves attendues manquent pour répondre au point de contrôle.
- **Défaillant** : aucune preuve attendue n'est disponible pour répondre au point de contrôle.

Exemple d'échelle à six niveaux :

- **Optimisé** : les pratiques sont formalisées, mises en œuvre, contrôlées et améliorées de façon continue.
- **Maîtrisé** : les pratiques sont formalisées, mises en œuvre, mais non contrôlées ou non améliorées de façon continue.
- **Défini** : les pratiques sont formalisées et globalement mises en œuvre.
- **Reproductible** : les pratiques sont régulièrement mises en œuvre, non formalisées ou partiellement appliquées.
- **Initial** : existence de pratiques informelles.
- **Défaillant** : pratiques inexistantes.

Cette évaluation permet de révéler précisément les points de faiblesse et d'orienter les actions correctives nécessaires.

Le plan de contrôle est un outil vivant qui doit être revu régulièrement. À titre d'exemple, une revue s'impose dans les situations suivantes :

- les résultats des contrôles de l'année N-1 ont été évalués comme défaillants/à améliorer ;
- des recommandations issues d'audits internes/externes ont été identifiées ;
- un ou des incidents sont survenus, mettant en exergue l'absence ou l'inefficacité d'un ou de plusieurs contrôles ;
- de nouvelles réglementations apparaissent dans le paysage réglementaire ;
- l'entreprise s'est réorganisée.

2.6 Plan de contrôle « cybersécurité »

2.6.1 Caractéristiques

Un plan de contrôle « cybersécurité » est propre à chaque entreprise, ceci afin de répondre précisément à ses besoins, à son niveau de maturité « cyber » et à son contexte unique.

Le plan de contrôle « cybersécurité » se doit d'être évolutif, c'est-à-dire d'être révisé a minima chaque année et d'être enrichi à mesure que l'entreprise connaît des changements techniques, réglementaires et/ou organisationnels ou des incidents/crises.

2.6.2 Exemples de thématiques pouvant être abordées dans le cadre d'un plan de contrôle cyber

- Gestion de la gouvernance « cybersécurité » : comitologie, tableaux de bord, communication aux dirigeants, rôles et responsabilités…
- Gestion de la continuité et reprise d'activité : durées d'interruption maximales admissibles, perte de données maximale admissible, existence de plans, réalisation de tests, sauvegardes et restauration…
- Gestion des crises « cyber » : politiques, plans et procédures afférentes…
- Gestion des identités et des accès logiques : attribution d'un identifiant unique et pérenne, gestion du cycle de vie (arrivées, mobilité, départ temporaire ou définitif), authentification, gestion des comptes (création, modification, suppression), gestion des habilitations (attribution, retrait), séparation des tâches (SoD)…
- Gestion sécurisée des actifs (logiciels et matériels) : acquisition ou développement d'actifs, déclaration dans le référentiel des actifs, installation, mises en production, décommissionnement, gestion et exploitation des actifs, gestion des configurations, gestion des traitements, gestion de la capacité et des performances…
- Gestion des évènements, des incidents et des problèmes : traçabilité / journalisation, mise en place d'alertes, traitement des anomalies incluant leur qualification et l'évaluation des impacts, engagements de services, retours d'expérience, récurrence des incidents…
- Gestion des vulnérabilités et de l'obsolescence : correctifs des systèmes d'exploitation, correctifs des logiciels, correctifs des applications, gestion de l'obsolescence (= gestion des systèmes legacy), maintien en condition de sécurité des actifs legacy…
- Gestion de la sécurité réseau : filtrage, segmentation, Wi-Fi, connexion sécurisée à distance, cartographie des flux, contrôles d'accès (NAC), réseau distinct et spécifique pour l'administration des actifs, séparation des environnements (production / hors production)…
- Sensibilisation et formation cybersécurité : régularité, bonnes pratiques de développement sécurisé, tests de phishing, intégration des nouveaux entrants incluant une sensibilisation à la sécurité…
- Gestion de la sécurité des données : protection de la disponibilité, de l'authenticité, de l'intégrité et de la confidentialité des données, prévention et détection des fuites de données, accords de confidentialité ou de non-divulgation, sécurité des données en transit, chiffrement sur la base de la classification des données et l'évaluation des risques, sélection des techniques cryptographiques, gestion des certificats.
- Gestion de la sécurité dans les projets : (ISP = intégration de la sécurité dans les projets), gouvernance, étapes, méthode de test, spécifications fonctionnelles et techniques, gestion des changements.

3 Liste des points d'attention et des prérequis

Ce chapitre examine les questions essentielles à poser pour la mise en œuvre d'un contrôle permanent de niveau 2. Il détaille les référentiels, les risques, la gestion des ressources, les processus cyber et la documentation nécessaire.

Ressources

- A-t-on les ressources humaines suffisantes ?
- Peut-on désigner un pilote pour le programme de contrôle permanent de niveau 2 cyber ?
- Le programme peut-il être soutenu financièrement par la direction ?
- Les acteurs du contrôle ont-ils les compétences nécessaires ?
- Quels sont les rôles et responsabilités de chacun des acteurs ? Un RACI est-il clairement défini ?

Processus et procédures

- Les processus/procédures cyber sont-ils identifiés ?
- Les processus/procédures cyber sont-ils correctement définis (objectifs clairs, données entrantes et sortantes précises, etc.) ?
- Des indicateurs d'efficacité des processus/procédures sont-ils en place ?
- Les processus/procédures cyber sont-ils documentés ?
- Y a-t-il un processus/procédure de suivi des plans d'action issus des différents contrôles ? Ce processus intègre-t-il bien une escalade en cas de non-mise en œuvre des actions dans les délais impartis ?
- La documentation des processus/procédures cyber est-elle revue régulièrement et mise à jour en conséquence ?
- Est-ce que les rôles et les responsabilités en ce qui concerne l'élaboration, la mise en œuvre et la maintenance des processus/procédures sont clairement définis ?

Documentation cyber

- Existe-t-il un corpus documentaire sur la sécurité des systèmes d'information, par exemple une échelle de classification des informations / documents ?
- Ce corpus est-il revu régulièrement et mis à jour en conséquence ?
- Le corpus documentaire a-t-il été communiqué à qui de droit ?
- Le corpus documentaire est-il connu des utilisateurs concernés, avec un accès facilité, dans sa bonne version ?
- Les utilisateurs concernés ont-ils signé les chartes ? Ces dernières font-elles l'objet d'une communication/sensibilisation à intervalle régulier ?
- Existe-t-il des NDA ?
- Les utilisateurs concernés ont-ils signé ces éventuelles NDA ?

Référentiels

- Quels sont les référentiels cyber internes applicables à l'entreprise ?
- Quels sont les référentiels cyber externes applicables à l'entreprise ?
- A-t-on accès aux contenus des référentiels externes applicables à l'entreprise ?
- A-t-on les ressources qualifiées pour analyser les référentiels internes et externes applicables à l'entreprise ?
- A-t-on les ressources qualifiées pour décliner opérationnellement les référentiels internes et externes applicables à l'entreprise ?

Risques

- Les principaux risques affectant l'entreprise sont-ils connus et évalués ?
- Le périmètre du contrôle couvre-t-il l'ensemble des risques identifiés (risques opérationnels, de non-conformité ou liés à la sécurité du SI) ?
- Un plan d'action est-il en œuvre pour réduire les principaux risques affectant l'entreprise ?
- Quelle est la notoriété de l'entreprise (B2B, B2C, nationale, internationale…) ?

Management et organisation

- Avez-vous des réglementations propres à votre entreprise ?
- La démarche est-elle appuyée par la direction générale ? Avez-vous des certifications à maintenir ?
- Les principaux interlocuteurs sont-ils identifiés pour la mise en œuvre des contrôles ?
- Y a-t-il une matrice des responsabilités (RACI) des contrôleurs de niveau 2 en place ?
- Existe-t-il une séparation claire entre les niveaux de contrôle 1, 2 et 3 ?
- Le management opérationnel est-il sensibilisé à la charge associée à la mise en œuvre des contrôles ?
- Des comités de suivi et de restitutions sont-ils programmés ?
- Le plan de contrôle est-il partagé avec les futurs opérationnels contrôlés ?
- Existe-t-il des interactions avec d'autres fonctions (audit interne, risque, conformité) ?

4 Exemples de points de contrôle « cyber »

Ce chapitre présente divers exemples de contrôles pouvant être réalisés.

Il aborde les thématiques de :

- gouvernance,
- conformité légale et réglementaire,
- gestion des identités et des accès,
- continuité et gestion de crise,
- gestion des actifs,
- protection de l'information,

pour aider les lecteurs à structurer les contrôles cyber.

Nota bene :

Comment distinguer une mesure d'un contrôle ?

> Pour distinguer une mesure d'un contrôle, il faut passer d'une question d'existence de l'outil, du document, de l'action, etc., à une question de vérification de la mise en œuvre et de l'efficacité (de l'outil, du document, de l'action, etc.).

Comment distinguer un contrôle de niveau 1 d'un contrôle de niveau 2 ?

> Un contrôle de niveau 1 consiste à vérifier la bonne exécution quotidienne ou hebdomadaire de la mesure. Si le contrôle n'est pas fait, l'opération s'arrête ou échoue.
>
> Un contrôle de niveau 2 va plus loin : c'est un contrôle de supervision périodique (mensuel, trimestriel ou annuel) Il s'assure de la conformité et de l'efficacité du dispositif, notamment par échantillonnage et par la vérification de l'existence, de la réalité et de la pertinence des contrôles de niveau 1. Si le contrôle de niveau 2 n'est pas fait, cela n'a pas d'impact sur l'opération en elle-même, mais elle n'est peut-être pas réalisée de manière optimum ou fiable.

4.1 Gouvernance

Dispositif/Mesure	Contrôle de niveau 1	Contrôle de niveau 2
Existe-t-il une stratégie cybersécurité ?	Vérifier que la stratégie cyber est formalisée et validée au bon niveau	Contrôler que la stratégie est revue annuellement et alignée sur la stratégie globale de l'entreprise
Existe-t-il une charte informatique ?	Vérifier la diffusion de la charte Vérifier que chaque nouvel arrivant a signé la charte	Pour un échantillon, contrôler la complétude du processus de signature
Existe-t-il des supports de formation cyber ?	Vérifier que les supports de formation intègrent les risques cyber	Contrôler les émargements des sessions Contrôler le taux d'appropriation des notions
Existe-t-il un corpus documentaire cyber (PSSI et/ou politiques thématiques ?	Vérifier que le corpus documentaire cyber est mis à jour à chaque changement majeur organisationnel, architectural, réglementaire ou, a minima, annuellement Vérifier que le corpus documentaire est diffusé	Contrôler que le responsable documentaire produit un rapport trimestriel de suivi des révisions et que les alertes de retard ont été traitées Contrôler que la PSSI a bien été révisée à la suite de la mise en application d'une nouvelle réglementation (DORA, NIS…), d'un changement de nom de l'entreprise, etc. Contrôler que la revue a été validée au bon niveau Contrôler que les collaborateurs disposent bien de la dernière version du corpus documentaire
Existe-t-il un poste / une fonction de responsable de la sécurité des systèmes d'information ?	Vérifier qu'une fiche de poste / fonction existe et que le poste / la fonction est bien occupé au sein de l'entreprise	Examiner les missions réalisées par la personne en place : sont-elles conformes à la fiche de poste / fonction ?

Existe-t-il une sensibilisation cyber (phishing, etc.) ?	Vérifier que des actions de sensibilisation ont été réalisées Vérifier que les évaluations ont été remplies Analyser le niveau d'appropriation des personnes sensibilisées à travers les résultats du questionnaire	Contrôler que les résultats des actions de sensibilisation ont été analysés en comité de sécurité et que d'éventuels plans d'action correctifs ont été validés pour les populations ayant échoué
Existe-t-il des comités cyber (COSEC, etc.) ?	S'assurer de la présence d'un ordre du jour et d'un compte-rendu pour chaque instance	Contrôler que les décisions stratégiques actées en comité et mentionnées dans le CR sont effectivement transformées en actions et suivies
Existe-t-il un RACI ?	Vérifier que les rôles et responsabilités cyber sont bien définies (RSSI, DSI, Direction, etc.)	Contrôler que les rôles et responsabilités correspondent bien aux missions ou aux fiches de poste
Existe-t-il des clauses « cyber » et plans d'assurance sécurité dans les contrats avec les tiers	Construire une check-list de vérification « clause cyber » à intégrer dans chaque nouveau contrat signé	Réaliser un audit sur un échantillon pour vérifier la présence et la validité des clauses de la check-list
Existe-t-il un système de stockage de preuves des contrôles ?	Vérifier que les preuves sont systématiquement enregistrées dans l'outil dédié après chaque contrôle	Tester l'intégrité et l'accessibilité d'un échantillon de preuves sur une période donnée
Existe-t-il un *reporting* des contrôles ?	Vérifier que les contrôles mis en place ont abouti à un rapport a minima annuel	Vérifier que le rapport a bien été envoyé à la Direction et qu'il montre bien le taux de couverture des contrôles

4.2 Conformité légale et réglementaire

Dispositif/Mesure	Contrôle de niveau 1	Contrôle de niveau 2
Existe-t-il un dispositif de veille réglementaire ?	Vérifier l'existence d'une procédure formalisant la lecture mensuelle du JOE, des décrets, etc., et la communication en découlant	Vérifier qu'une nouvelle réglementation a bien donné lieu à une analyse d'impact et à une communication interne telle que documentée
Existe-t-il un recensement à jour des obligations légales en matière de cybersécurité ?	Vérifier qu'une preuve de la révision (date/visa) du registre des obligations est bien présente et récente (moins de 6 mois, par ex.)	Contrôler si la nouvelle loi (ex. : DORA, AI Act) a bien été intégrée au registre dans les délais impartis
Existe-t-il une classification des obligations légales en matière de cybersécurité ?	Vérifier que chaque nouvelle obligation est affectée à une catégorie du référentiel	S'assurer de la cohérence globale du classement pour permettre un *reporting* consolidé
Existe-t-il des mesures de sensibilisations réglementaires ?	Comparer le contenu pédagogique des sensibilisations avec la liste des obligations réglementaires	Contrôler le taux de complétion des formations et le taux de validation des acquis
Existe-t-il des contrôles périodiques de conformité réglementaire du SI et des pratiques ?	Vérifier que chaque contrôle de la conformité réglementaire des pratiques et des SI réalisé est consigné dans un journal de bord avec les résultats obtenus	Vérifier que 100 % des contrôles prévus dans le plan annuel ont été réellement exécutés et documentés
Existe-t-il un plan d'action suivi/piloté de mise en conformité réglementaire ?	Pour chaque non-conformité détectée, vérifier l'existence d'un ticket de suivi avec un responsable et une échéance	Analyser la pertinence des plans d'action proposés Analyser le taux de retard des plans d'action et alerter la Direction en cas de dérive majeure

4.3 Gestion des identités et des accès

Dispositif/Mesure	Contrôle de niveau 1	Contrôle de niveau 2
Y a-t-il attribution d'un identifiant personnel unique et pérenne aux utilisateurs ?	Vérifier que l'identifiant n'est pas déjà attribué	Contrôler, sur un échantillon de l'annuaire des identifiants, qu'il n'y a pas de doublon Contrôler que l'identifiant sert à une personne physique et n'est pas partagé
Existe-t-il des comptes de service ?	Vérifier qu'un responsable est nommé pour chaque compte de service	Contrôler le registre des comptes de service pour vérifier qu'aucune dérogation n'a été accordée sans analyse de risque préalable
Comptes de secours	Vérifier la présence d'une enveloppe scellée dans le coffre-fort	Contrôler le registre d'accès au coffre-fort pour s'assurer qu'aucune ouverture n'a eu lieu sans ticket d'incident associé
Existe-t-il un processus de création, modification et suppression des accès ?	Vérifier que chaque demande d'accès fait l'objet d'un ticket tracé avec une preuve d'approbation managériale	Contrôler mensuellement que 100 % des comptes créés correspondent à un ticket validé
Existe-t-il une revue des comptes et droits par les managers et propriétaires d'actif ?	Vérifier la réalisation effective de la campagne de revue par le manager et/ou le propriétaire d'actif / vérifier que chaque manager a bien signé son compte-rendu de revue	Contrôler la qualité de la revue : vérifier que la revue est exhaustive Contrôler qu'aucun compte ou droit « dormant » n'a été maintenu actif inutilement
Existe-t-il une séparation des tâches ? Existe-t-il une limitation des droits au strict nécessaire (moindre privilège) ?	Analyser (automatiquement ou manuellement) les droits attribués et identifier les cumuls incompatibles	Contrôler la cohérence : vérifier que les droits d'un échantillon d'utilisateurs correspondent réellement à leurs fiches de poste et qu'il n'y a pas de droits incompatibles attribués Contrôler que l'outil de gestion des droits bloque automatiquement les combinaisons toxiques

Existe-t-il une journalisation des évènements de gestion des identités et des habilitations ?	Vérifier les alertes ou rapports d'erreurs	Contrôler (trimestriellement, par ex.) que les logs sont bien intègres, stockés selon la durée légale et non modifiables
Existe-t-il un traitement spécifique des comptes à privilèges ?	Vérifier que les comptes à privilèges sont bien inventoriés et recertifiés régulièrement	Contrôler l'usage des comptes à privilèges uniquement dans les fenêtres d'intervention prévues
Est-ce que les comptes à privilèges ne sont utilisés qu'à des fins d'administration ?	Vérifier, via les logs, que les administrateurs n'utilisent pas leur compte à privilèges pour des actes standards (traitement mail, navigation web)	Contrôler trimestriellement, pour un échantillon d'administrateurs, qu'ils n'ont pas réalisé d'actes standards avec leur compte à privilèges Contrôler que les alertes « utilisation d'un compte à privilèges pour un acte standard » sont toutes suivies d'effets Réaliser un audit de configuration pour valider l'étanchéité réelle entre les comptes standards et privilégiés
Existe-t-il une authentification forte pour les accès distants et les fonctions critiques ?	Vérifier la configuration technique systématique du MFA pour tout nouvel accès distant ou sensible	Contrôler les comptes qui auraient « bypasser » le MFA
Existe-t-il un processus de clôture ou d'adaptation des accès lors des mouvements RH ?	Vérifier que les accès ont été désactivés dans le délai imparti (24 heures après la notification RH, par ex.)	Faire un rapprochement entre la liste des départs RH du mois et la liste des comptes supprimés/désactivés

4.4 Continuité et gestion de crise

Dispositif/Mesure	Contrôle de niveau 1	Contrôle de niveau 2
Existe-t-il un responsable du plan de continuité d'activité (RPCA) désigné ?	Vérifier que le RPCA a clairement été identifié Vérifier qu'une fiche de poste/fonction a été établie	Contrôler que la lettre de mission est validée et revue périodiquement par la Direction Contrôler que les missions sont bien exécutées
Existe-t-il une gouvernance PCA ?	Vérifier que des comités PCA sont tenus selon la fréquence prévue	Contrôler que 100 % des comités ont donné lieu à un compte-rendu avec un relevé de décisions suivies
Existe-t-il une stratégie de continuité d'activité ?	Vérifier que le document est validé par la Direction	Contrôler la bonne diffusion du document, son accessibilité à tous les acteurs concernés Contrôler qu'il n'y a pas de version obsolète en circulation
Existe-t-il un planning de test de résilience ?	Vérifier qu'un planning annuel de test a été établi	Contrôler que le programme de test a été validé Contrôler que le planning est respecté
Existe-t-il des indicateurs concernant la continuité d'activité ?	Vérifier que les indicateurs sont alimentés en temps et en heure	Contrôler la pertinence / l'utilité des indicateurs proposés
Existe-t-il un Business Impact analysis (BIA) ?	Vérifier que chaque direction métier a validé ses RTO/RPO	Contrôler que le BIA est mis à jour annuellement Contrôler que la méthodologie de calcul des impacts est cohérente avec la politique de gestion des risques de l'entreprise Contrôler que l'arbitrage des priorités a bien été validé par la Direction

Existe-t-il un Plan de continuité d'activité (PCA) à jour ?	Vérifier qu'un PCA a formellement été décrit pour les activités mentionnées dans la stratégie (activités critiques, par ex.) Vérifier que la PCA couvre bien les scénarios mentionnés dans la stratégie	Contrôler que toutes les activités critiques font bien l'objet d'un PCA Contrôler que le PCA est revu à chaque évolution organisationnelle ou technologique de l'entreprise ou a minima annuellement
Existe-t-il un corpus documentaire du Plan de Secours informatique (PSI) à jour ?	Vérifier après chaque changement majeur que la documentation technique est à jour	Contrôler qu'une nouvelle évolution architecturale a bien été prise en compte
Existe-t-il des tests du Plan de Secours informatique (PSI) ?	Vérifier qu'un compte-rendu après chaque test est rédigé Vérifier qu'un suivi des anomalies est réalisé	Contrôler que les plans d'action issus des tests sont clôturés dans les délais impartis Contrôler la pertinence des arbitrages des priorités de remédiation Contrôler que les plans d'action proposés sont pertinents
Existe-t-il des sauvegardes ?	Vérifier chaque matin le rapport des sauvegardes (succès/échecs) Vérifier qu'une restauration est possible	Contrôler trimestriellement que 100 % des rapports d'échec de sauvegarde ont généré un ticket d'incident Contrôler que des tests de restauration complète (avec validation métier) ont été faits
Les sauvegardes sont-elles envoyées sur un site distant ?	Vérifier la bonne réplication des sauvegardes sur le site secondaire	Contrôler l'étanchéité des deux sites (primaire et secondaire)
Existe-t-il une sensibilisation à la continuité d'activité ?	Vérifier que les supports de sensibilisation sont à disposition Vérifier que les sessions de sensibilisation sont émargées Vérifier le suivi formalisé de la sensibilisation à la continuité d'activité (planning, couverture, etc.)	Contrôler, sur un échantillon de collaborateurs, le niveau de connaissance du PCA Contrôler trimestriellement que 100 % des nouveaux acteurs clés ont été formés Contrôler que les indicateurs de sensibilisation sont présentés et validés par la Direction

Existe-t-il une documentation de gestion de crise ?	Vérifier l'annuaire des personnes à prévenir en cas de crise Vérifier la check-list d'urgence Vérifier les messages types préparés	Contrôler que toutes les parties prenantes sont bien mentionnées Contrôler que l'annuaire est régulièrement révisé Contrôler que la check-list est revue après les tests Contrôler que la communication de crise a bien été validée par la direction de la communication
Existe-t-il des cellules de crise ?	Vérifier que les comptes-rendus des tests de mobilisation des acteurs sont formalisés	Contrôler l'efficacité de la mobilisation par retour d'expérience

4.5 Gestion des actifs

Dispositif/Mesure	Contrôle de niveau 1	Contrôle de niveau 2
Existe-t-il un politique de gestion des actifs à jour ?	Vérifier que la politique est formalisée	Contrôler que la politique a été validée par la Direction Contrôler que la politique est appliquée (que des processus et des procédures permettent de la décliner formellement, que les pratiques de gestion des actifs sont conformes à la politique) Contrôler la diffusion et l'accessibilité à travers un recueil de la version connue des parties prenantes
Existe-t-il un processus de mise à jour du référentiel des actifs ?	Vérifier que les actifs sont saisis dans le référentiel des actifs lors de leur acquisition, lorsqu'ils subissent un changement ou lors de leur décommissionnement	Contrôler l'exhaustivité du référentiel des actifs en rapprochant le référentiel des achats, le résultat d'un scan du réseau, etc., avec le référentiel des actifs Contrôler pour un échantillon que le statut de l'actif est conforme à la réalité
Existe-t-il un référentiel des actifs correctement rempli et à jour ?	Vérifier que tous les champs sont correctement saisis Vérifier que le champ RTO/RPO est renseigné Vérifier que les actifs sont classés conformément à la politique	Contrôler que des indicateurs de qualité du référentiel ont été mis en place et sont suivis (donne lieu à des remédiations) Contrôler que le champ RTO/RPO du référentiel est cohérent avec le BIA Contrôler la cohérence globale de la classification
Existe-t-il un propriétaire pour chacun des actifs ?	Vérifier que chaque actif possède un responsable désigné	Contrôler, pour un échantillon d'actifs, que le propriétaire est le bon, n'a pas quitté l'entreprise ou n'a pas changé de fonction

Existe-t-il un processus / une procédure de restitution des terminaux utilisateurs au départ d'un collaborateur ?	Vérifier que la check-list de départ confirmant la remise des terminaux a bien été signée par le manager Vérifier que le statut des actifs a bien été mis à jour dans le référentiel	Contrôler mensuellement la liste des départs avec la liste des attestations de restitution signées Contrôler le taux de restitution des actifs (comparaison entre la liste des attestations et le référentiel des actifs) Contrôler que les incidents de restitution sont bien documentés et suivis
Existe-t-il des indicateurs de gestion des actifs ?	Vérification du suivi opérationnel des indicateurs	Contrôler l'utilisation des indicateurs pour arbitrer

Protection de l'information

Dispositif/Mesure	**Contrôle de niveau 1**	**Contrôle de niveau 2**
Existe-t-il une politique de protection de l'information documentée ?	Vérification de l'existence et de l'actualité de la politique	Contrôler l'approbation par la Direction
Existe-t-il des exigences métier en termes de confidentialité, intégrité et disponibilité ?	Vérifier la prise en compte des exigences de confidentialité, intégrité et disponibilité dans les projets	Contrôler, pour un échantillon, la formalisation du besoin métier dans les documents projets
Existe-t-il des mesures de sécurité définies par niveau de classification ?	Vérification de la configuration des outils DLP (Data Loss protection) conformément à la politique	Contrôler la cohérence globale des mesures en fonction du niveau de classification
Existe-t-il des outils de protection contre les activités malveillantes à jour ?	Vérifier que tous les systèmes disposent d'une protection Vérifier que les bases de détection des agents sont à jour	Contrôler l'exhaustivité de la couverture en comparant le référentiel des actifs avec la base de l'EDR/XDR Contrôler l'indicateur de mise à jour
Existe-t-il une liste de logiciels approuvés ?	Vérifier la conformité des installations par rapport à la liste	Contrôler si les exceptions sont validées au bon niveau
Existe-t-il un filtrage web ?	Vérifier que les règles de filtrage soient bien opérationnelles	Contrôler que les règles ont été validées

Existe-t-il un chiffrement des données ?	Vérifier que le chiffrement est activé dans la configuration d'une nouvelle base de données	Contrôler, avec une campagne de scan, que les flux de données sont chiffrés selon les standards Contrôler que les standards de chiffrement utilisés ont été validés par le RSSI
Existe-t-il des règles de conservation formalisées ?	Vérifier que les règles sont respectées	Contrôler la conformité réglementaire des durées de conservation implémentées
Existe-t-il une surveillance des fuites de données ?	Vérifier les alertes et incidents DLP	Contrôler les rapports d'incidents du DLP pour identifier les contournements ou les erreurs de *tagging*
Existe-t-il des tests d'intrusion ?	Vérifier la réalisation des tests selon le plan Vérifier la documentation des tests	Contrôler que les résultats ont été présentés et arbitrés par la Direction
Existe-t-il des rôles et responsabilités autour de la gestion des vulnérabilités ?	Vérifier l'existence d'un RACI	Contrôler la couverture des rôles Contrôler la validation du RACI par la Direction
Existe-t-il une veille sur les vulnérabilités ?	Vérifier l'abonnement et la réception effective à travers l'ouverture de ticket	Contrôler qu'une alerte majeure de l'ANSSI a bien donné lieu à une analyse d'impact et à une remédiation
Existe-t-il une procédure de classification des vulnérabilités ?	Vérifier que les vulnérabilités sont classées et traitées en conséquence Vérifier que les délais de traitement sont respectés	Contrôler la cohérence des classifications Contrôler que la classification est validée par le RSSI Contrôler les écarts de traitement et leur validation par la Direction

Existe-t-il des procédures de remédiation rapide ?	Comparer la date de découverte de la vulnérabilité avec la date de clôture du ticket de demande de remédiation pour calculer le délai de remédiation Vérifier, pour un ticket précis, que le correctif a bien été appliqué (PV recette)	Contrôler que le délai de remédiation est conforme aux exigences Contrôler que les dépassements ont été escaladés
Existe-t-il des scans de vulnérabilité ?	Vérifier que les scans ont bien été lancés et se sont terminés sans erreur	S'assure que le plan de scan annuel couvre 100 % du parc ou que ce qui n'est pas scanné est justifié par une analyse de risque
Existe-t-il une procédure de gestion des incidents de sécurité ?	Vérification du traitement et de la qualification des incidents	Contrôler les comptes-rendus d'incident et les arbitrages
Existe-t-il une sensibilisation à la protection de l'information ?	Vérification des actions de formation (contenu, planification, couverture, etc.)	Contrôler l'efficacité à travers le taux de compréhension

5 Retour d'expérience des membres du groupe de travail

Ce chapitre offre un retour d'expérience détaillé sur la mise en œuvre et la gestion d'un projet de contrôle cyber. Il analyse les défis rencontrés, les facteurs de réussite et les dynamiques internes qui ont facilité le processus.

Les bénéfices observés incluent :

- une meilleure gestion des anomalies ;
- une acculturation aux enjeux de la gestion du risque (et en particulier des risques cyber) ;
- une meilleure gestion des risques cyber.

5.1 Mise en œuvre du projet

- Quel a été le contexte de mise en œuvre du plan de contrôle ?
    - Réglementation, obligation réglementaire, volonté d'obtenir une certification (ISO 27001, PCI-DSS), adresser un marché US, UK, EU (ISAE, SOC 2…).
    - Contrôler les mesures de sécurité en l'absence de liens hiérarchiques.
    - Vérifier le déclaratif des équipes.
    - Dans le cadre d'obtention de financements, appuyer le ROI.
- Quels éléments du référentiel vous ont semblé les plus complexes ?
    - Résistance au changement des équipes.
    - Nécessité de formaliser les process, les procédures de contrôle…

5.2 Quels ont été les facteurs de réussite de la mission ?

- Sponsoring réel/concret de la Direction.
- La maîtrise du domaine par les équipes du contrôle permanent.
- Faire comprendre l'intérêt de la mission, en quoi elle peut aider les équipes.
- Ressources vraiment disponibles pour répondre.
- Communication claire sur la fréquence des contrôles.
- Communication sur le rôle de l'équipe du contrôle permanent et sur les finalités de la mission.
- Identification d'un référent qui puisse être l'« allié » du contrôleur.

5.3 Quelles dynamiques internes ont facilité le déroulement de la mission ?

- Implication des équipes et services audités.
- Démarche d'accompagnement au changement.

5.4 Quelles ont été les principales difficultés rencontrées ?

- Difficulté à établir des KPI pérennes.
- Difficulté à communiquer avec des profils experts, si le contrôleur n'a pas le bagage/qu'il n'y a pas de « traducteur ».
- Question de la légitimité du contrôleur face aux équipes.
- Difficulté de compréhension du bien-fondé de la mise en place du plan de contrôle.

5.5 Quelles sont les évolutions envisagées ?

- Formuler des contrôles plus proches des pratiques métier.
- Établir une feuille de route évolutive, donner de la visibilité (ce qui sera fait l'année prochaine, par ex.) et laisser du temps.

5.6 Quels ont été les bénéfices observés ?

- Permettre aux opérationnels de s'approprier les enjeux de la gestion du risque, les acculturer à ces aspects.
- Facilitation des transferts de connaissance (remplacement, recrutement) grâce à la documentation réalisée lors des contrôles.
- Maintien d'une façon de faire uniforme/régulière et donc de métriques comparables.
- Détection plus simple des problématiques/anomalies, car les process et outils sont mieux connus.

5.7 Conseils à une organisation qui démarre la mise en œuvre d'un projet similaire ?

- Adoptez une mise en place progressive des contrôles, en fonction de la maturité de l'organisation. Mettre en place quelques contrôles, établir de premiers indicateurs automatisés et enrichir le plan.
- Le périmètre des contrôles doit être défini dès le départ.
- Identifiez précocement les bons interlocuteurs.
- Lors du lancement du projet, misez fortement sur la pédagogie, davantage que sur le jugement.
- Veillez à ce que les éventuelles recommandations ne donnent pas lieu à des compréhensions erronées/partielles/déstabilisantes.

6 Les mots du contrôle permanent

Afin d'élaborer une approche méthodologique précise, il est essentiel de définir clairement les termes utilisés en contrôle permanent.

6.1 Les acronymes

AC : Activité de contrôle

AIC : Activité importante et critique

BIA : Business Impact Analysis

CPN1 / CPN2 : Contrôle permanent de niveau 1 / Contrôle permanent de niveau 2

DLP : Data Loss Protection

DMR : Dispositif de maîtrise des risques

DORA : Digital Operational Resilience Act

DPO : Délégué à la Protection des Données (*Data Protection Officer*)

EDC : Environnement de contrôle

FIC : Fonction importante et critique

LCB-FT : Lutte contre le blanchiment de capitaux et le financement du terrorisme

NIS : Network and Information Security

OCS : Officier central de Sécurité

PCA : Plan de continuité d'activité

PCI : Plan de continuité informatique

PRA : Plan de reprise d'activité

PRI : Plan de reprise informatique

PSI : Plan de Secours informatique

RGPD : Règlement général sur la Protection des Données

RSSI : Responsable Sécurité des Systèmes d'information

SIEM : Security Information and Event Management

SOC : Security Operation Center

SSI : Sécurité des Systèmes d'Information

TIC : Technologies de l'information et de la communication

6.2 Les termes à ne pas confondre

Le groupe de travail propose plusieurs groupes de termes et expressions qui font l'objet d'une confusion régulière :

- Actif (Asset) : Ressource ayant de la valeur pour une organisation (données, systèmes, applications, infrastructures).
- Actif informationnel : Ensemble des informations (matérielles ou immatérielles) d'une organisation.
- Actif de TIC : Actif logiciel ou matériel dans les réseaux et les systèmes d'information utilisés par une entité / une organisation.

*

- Activité importante et critique : Ensemble de tâches ou de processus opérationnels dont le bon déroulement est vital pour la continuité des activités d'une organisation. Activité dont l'interruption ou la dégradation aurait un impact majeur (financier, réglementaire, opérationnel ou réputationnel).
- Fonction importante et critique : Fonction pouvant être composée de plusieurs activités importantes et critiques. C'est un niveau d'abstraction plus élevé que l'AIC. Exemple : la fonction « Gestion des paiements » est une fonction importante et critique. Elle regroupe plusieurs activités importantes et critiques, comme le traitement des transactions, la détection des fraudes, la compensation interbancaire, etc.

*

- Plan de continuité d'activité : C'est un plan qui a une portée globale et orientée métier. Son objectif est d'assurer la continuité des fonctions et processus les plus critiques de l'entreprise en cas d'incident majeur (ex. : indisponibilité de l'informatique). Le PCA ne se limite pas aux aspects techniques. Il couvre l'ensemble des ressources nécessaires (humaines, procédures manuelles à suivre, site de repli, transport… et informatique).
- Plan de continuité informatique : C'est un plan orienté technologie. Il vise à garantir la disponibilité et la résilience du système d'information. C'est un sous-ensemble du plan de continuité d'activité.

*

- Sécurité de l'information : C'est l'ensemble des mesures techniques, organisationnelles, humaines et physiques mises en place pour protéger les informations (matérielles ou numériques) d'une organisation. Son objectif principal est de garantir trois propriétés fondamentales de l'information : la confidentialité, l'intégrité et la disponibilité[3].
- Cybersécurité : C'est la protection des systèmes informatiques (ordinateurs, serveurs, réseaux, etc.) et des informations numériques contre les attaques, les dommages ou les accès non autorisés. C'est le sous-domaine de la sécurité de l'information qui se concentre spécifiquement sur la dimension numérique et électronique.

*

- Système d'information : C'est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information au sein d'une organisation : cela comprend aussi bien les systèmes informatiques (avec lesquels il ne faut pas le confondre) que les informations, qu'elles soient sous format numérique ou papier.
- Système informatique : C'est un sous-ensemble technique du système d'information. Il regroupe les moyens matériels (ordinateurs, serveurs, réseaux, périphériques, stockage) et logiciels (systèmes d'exploitation, logiciels/applications) qui permettent de faire fonctionner le système d'information.

[3] La traçabilité est importante pour la sécurité de l'information, mais elle ne fait pas partie des propriétés fondamentales traditionnelles (triade CIA). C'est une propriétaire secondaire qui est un pilier de l'intégrité et de la non-répudiation.

- Mesure : Action, outil, politique, procédure, règle mise en place et destinée à réduire un risque, à prévenir un incident, à éviter une menace ou à limiter un impact.
- Contrôle : Mécanisme qui permet de s'assurer que la mesure est mise en œuvre, appliquée, maintenue et qu'elle fonctionne correctement.

Caractéristique	Mesure (Dispositif)	Contrôle (Vérification)
Rôle	Protéger/Prévenir	Confirmer/Détecter les failles
Question posée	Qu'est-ce qu'on fait pour réduire le risque ?	Est-ce qu'on fait ce qu'on a dit qu'on ferait ?
Temporalité	Permanente (en continu)	Ponctuelle ou périodique
Exemples concrets	Mettre un cadenas sur une porte (l'action pour éviter une visite importune) C'est la limitation de vitesse à 80 km/h (l'action pour réduire le risque d'accident)	Vérifier tous les soirs que le cadenas est bien en place et fermé (la vérification que la mesure est efficace) C'est le radar au bord de la route (la vérification que la mesure est bien respectée)

A noter : une mesure sans contrôle est « aveugle » (on espère que ça marche, mais on n'en est pas sûr). Un contrôle sans mesure est inutile (on vérifie quelque chose qui n'existe pas).

*

- Contrôle interne : Dispositif global mis en place par une entreprise pour maîtriser ses activités.
- Contrôle permanent : Une des deux composantes principales du dispositif global de contrôle interne (l'autre étant le contrôle périodique / l'audit interne).

6.3 Glossaire

- **Analyse de risques** : Méthode pour identifier, évaluer et prioriser les risques, dans le but d'orienter les décisions, telles que les mesures à mettre en œuvre, les délais à respecter, les responsables. Il existe des méthodes d'analyse de risque reconnues, telles que EBIOS RM, ISO 27005, NIST SP 800-30, FAIR, OCTAVE, MEHARI.
- **Approbation** : Autorisation formelle d'une opération.
- **Activité de contrôle** : Cela désigne les politiques, les procédures et les outils de vérifications mis en place pour prévenir ou réduire les risques susceptibles de nuire à l'atteinte des objectifs d'une organisation. Elle sert à prévenir, détecter ou corriger des vulnérabilités, des erreurs ou des fraudes. Elle peut être manuelle ou automatisée. Sa nature peut être de nature :
  - préventive : elle vise a empêcher un incident de sécurité (ex. : séparation des tâches (SoD), contrôles d'accès, etc.) ;
  - détective : elle est conçue pour identifier et signaler un incident de sécurité en cours (ex. : audits de sécurité, audits internes, rapprochement entre la liste du personnel et les comptes d'une application, etc.) ;
  - corrective : elle limite l'impact d'un incident de sécurité une fois qu'il s'est produit (ex. : restauration de données).
- **Contrôle** : Ensemble des mécanismes de vérification (manuels ou automatiques) des processus, procédures et autres mesures mises en place, notamment pour prévenir et réduire les risques. Les contrôles assurent une maîtrise des activités, garantissent la protection et la sauvegarde du patrimoine informationnel, ainsi que la conformité par rapport aux référentiels applicables (lois, règlements…). Le contrôle apporte la preuve que la maîtrise du risque est réelle.
- **Contrôle clé** : Contrôle/vérification essentiel(le) pour réduire un risque.
- **Corpus documentaire** : Collection structurée de documents réunis pour répondre à une question ou un usage, avec des règles claires de sélection, d'organisation et d'accès (stratégies, politiques, procédures, chartes, plans, processus…).
- **Cyberattaque** : Action malveillante menée par un individu (hacker), un groupe cybercriminel, une organisation étatique ou un programme automatisé (malware) pour exploiter une vulnérabilité (faille ou erreur) du système d'information d'une organisation. Action visant à compromettre la confidentialité, l'intégrité ou la disponibilité des données ou des systèmes informatiques.
- **Dispositif de maîtrise des risques** : Processus visant à identifier, analyser (priorisation, qualification), traiter les risques, en déployant des stratégies de réponse adaptées. Ce dispositif est essentiel dans le cadre de la gouvernance et du contrôle interne.
- **Environnement de contrôle** : Socle qui englobe les valeurs, les compétences des employés et la structure organisationnelle qui favorisent un comportement intègre et conforme.
- **Erreur** : Action involontaire entraînant une conséquence négative.
- **Fraude** : Action intentionnelle visant à obtenir un avantage indu.
- **Incident de sécurité** : Évènement avéré impactant la confidentialité, l'intégrité ou la disponibilité.
- **Malware :** Contraction de *Malicious Software*, il désigne tout programme ou code malveillant conçu pour infiltrer, perturber, endommager ou prendre le contrôle d'un système informatique, d'un réseau ou d'un appareil sans le consentement de l'utilisateur.
- **Menaces** : Tout élément pouvant potentiellement nuire / causer un dommage à l'activité de l'organisation en exploitant une ou des vulnérabilités.
- **Mesure :** Action, ou mécanisme mis en œuvre pour réduire un risque, renforcer un dispositif ou se conformer à des exigences spécifiques. Une mesure peut être de nature préventive, détective, corrective ou dissuasive, et peut inclure des outils techniques, des processus organisationnels ou des pratiques humaines (formation, sensibilisation). Elle agit directement sur la probabilité ou l'impact d'un risque.

- **Mesure de cybersécurité** : Mesure visant à protéger le Système d'information. Elles sont de trois types :
  - techniques (pare-feu, antivirus, chiffrement, etc.) ;
  - humaines et organisationnelles : sensibilisation, formation, politiques, procédure, etc. ;
  - physiques : contrôles d'accès physiques, surveillance des locaux.
- **Point de contrôle** : Un point de contrôle désigne un emplacement, une étape ou une instance de vérification prédéfinie dans un processus, un système d'information ou une architecture de sécurité. Il a pour finalité de détecter, prévenir ou corriger les écarts susceptibles de compromettre la maîtrise des risques, la protection du patrimoine informationnel, la continuité des activités, ainsi que la conformité aux exigences légales, réglementaires et normatives.
- **Preuve** : Trace formalisée des contrôles réalisés.
- **Processus** : Un processus est une suite de tâches / activités / opérations interdépendantes ou interactives visant à atteindre un objectif ou à produire un résultat. Un processus décrit un flux global de tâches (« quoi faire ») et la manière dont elles sont liées entre elles pour atteindre un but. Il formalise les flux d'informations, les interactions entre différentes entités, et les ressources mobilisées pour obtenir un résultat final. Un processus cherche à transformer des éléments (intrants) pour produire des résultats (extrants), en coordonnant diverses activités. Ces dernières peuvent parfois être ajustées en fonction des circonstances, tant que le résultat final est atteint.
  - Exemples de processus :
    - un processus de gestion des ressources humaines pourrait inclure des activités comme le recrutement, la formation, l'évaluation des performances ;
    - un processus de développement logiciel pourrait inclure la conception, le codage, les tests et la mise en production.
- **Procédure** : Document contenant un ensemble d'instructions détaillées qui décrit la manière de réaliser une tâche ou une activité. La procédure est une formalisation du savoir-faire de l'entreprise. Son but est d'assurer que les tâches complexes ou sensibles sont réalisées de manière standardisée, efficace et reproductible, quel que soit l'opérateur.
- **Réconciliation** : Comparaison de deux ensembles de données pour vérifier leur concordance.
- **Réglementation :** Ensemble de lois, normes, directives et obligations légales ou sectorielles qui imposent des exigences en matière de protection des systèmes d'information, de données et de services numériques. Ces règles visent à garantir un niveau minimum de sécurité, la résilience des infrastructures critiques et la protection des droits des individus.
- **Réponse à incident** : Ensemble des actions mises en œuvre pour contenir, éradiquer un incident, et récupérer de cet incident.
- **Résilience** : Capacité d'un système informatique (logiciel, matériel, réseau) à continuer à fonctionner ou à retrouver rapidement son état de fonctionnement normal en dépit d'évènements indésirables. Le concept de résilience va au-delà de la simple sécurité informatique ou du plan de reprise d'activité. C'est une approche globale qui intègre la prévention, la résistance et le rétablissement.
- **Risque** : Possibilité qu'un évènement indésirable survienne, entraînant un dommage, une perte ou un préjudice, et que cela ait un impact défavorable/négatif sur la réalisation des objectifs d'un organisme.
- **Risque lié aux TIC** : Toute circonstance raisonnablement identifiable liée à l'utilisation des réseaux et des systèmes d'information qui, si elle se concrétise, peut compromettre la sécurité des réseaux et des systèmes d'information, de tout outil ou processus dépendant de la technologie, du fonctionnement et des processus ou de la fourniture de services, en produisant des effets préjudiciables dans l'environnement numérique ou physique.

- **Risque inhérent** : Risque lié à la nature des activités d'un organisme.
- **Risque résiduel** : Risque qui persiste après la mise en place des mesures de sécurité.
- **SIEM** : Outil centralisant et corrélant les logs pour détecter les menaces.
- **SOC** : Équipe / centre responsable de la surveillance et de la détection des incidents de sécurité.
- **Système hérité ou Système legacy** : Système qui a atteint la fin de son cycle de vie (fin de vie), qui ne se prête pas à des mises à jour ou à des corrections, pour des raisons technologiques ou commerciales, ou qui n'est plus pris en charge par son fournisseur ou par un prestataire tiers de services TIC, mais qui est toujours utilisé et soutient les fonctions de l'entité / de l'organisation.
- **Vérification** : Examen des documents ou des opérations afin de s'assurer de leur exactitude.
- **Vulnérabilité** : Faiblesse ou défaut d'un actif, d'un système, d'un processus ou d'un contrôle qui, s'il est exploité par une menace, concrétise un risque et compromet le système d'information.



Tour Eria, 5 rue Bellini
92821 Puteaux Cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr