Exigence Thématique en matière de cybersécurité

Que sont les Exigences Thématiques?

Les Exigences Thématiques sont une composante essentielle du Cadre de référence international des pratiques professionnelles, qui comprend également les Normes internationales d'audit interne™ et les Lignes directrices internationales. L'Institute of Internal Auditors, en tant qu'organisme de normalisation de la profession d'audit interne, définit comme obligatoire ces Exigences Thématiques qui complètent les Normes internationales d'audit interne, qui font autorité pour les pratiques requises et qui sont décrites et référencées dans les Exigences Thématiques.

Les Exigences Thématiques fournissent une structure pour les sujets globaux fréquemment audités qui présentent généralement un risque plus élevé et sont de nature pervasives. Bien que les Normes s'appliquent à tous les services d'audit interne, une Exigence Thématique doit être considérée comme une exigence obligatoire supplémentaire à respecter lorsque le thème en question fait l'objet d'une mission d'audit interne.

Les Exigences Thématiques doivent être appliquées au niveau de l'entité ou de l'organisation sur des sujets qui ont un impact sur l'ensemble de l'organisation. Les auditeurs internes doivent connaître les Exigences Thématiques et être prêts à les mettre en œuvre lorsque le thème est inclus dans leurs plans d'audit annuels ou si ce thème spécifique fait l'objet d'une mission d'audit interne. Les éléments de l'Exigence Thématique doivent être évalués lors de la définition du périmètre de la mission. Les preuves que l'évaluation et le traitement du thème ont eu lieu doivent être documentées et conservées. Les missions qui incluent tout aspect relatif au thème doivent évaluer les exigences pertinentes pour la mission ou documenter les raisons pour lesquelles des exigences spécifiques ne sont pas applicables. Un outil destiné à aider les auditeurs internes à expliquer les raisons de l'inclusion ou de l'exclusion d'exigences est fourni à l'Annexe B.

Pourquoi les Exigences Thématiques sont-elles nécessaires ?

L'application des Exigences Thématiques vise à renforcer la pertinence de la fonction d'audit interne face à l'évolution du paysage mondial des risques et à accroître la valeur des services d'audit interne dans tous les secteurs d'activité. Le respect des Exigences Thématiques aidera les auditeurs internes à améliorer la qualité et la cohérence des missions.

Les Exigences Thématiques sont structurées de manière à fournir des orientations pour la réalisation de services d'audit interne dans trois domaines : la gouvernance, la gestion des risques et les processus de contrôle. Chaque domaine comprend :

- Les exigences, qui sont obligatoires et qui couvrent les objectifs essentiels de l'organisation.
- Les éléments à prendre en compte, qui ne sont pas obligatoires mais servent de bonnes pratiques pour évaluer la conception et la mise en œuvre des objectifs de l'organisation. Les éléments à prendre en compte, qui figurent à l'Annexe A, doivent être utilisées uniquement à titre d'exemples pour valider la conformité aux exigences.

La conformité aux Exigences Thématiques sera évaluée dans le cadre des évaluations de la qualité. Pour démontrer la conformité en vue d'unee évaluation de la qualité, les auditeurs internes doivent utiliser l'outil fourni à l'Annexe B pour indiquer la conformité à chaque exigence ou pour expliquer pourquoi la conformité n'est pas atteinte.

Exigence Thématique en matière de cybersécurité

Évaluation de l'efficacité des processus de gouvernance, de gestion des risques et de contrôle en matière de cybersécurité

La cybersécurité protège les actifs informationnels d'une organisation contre les utilisateurs non autorisés, les perturbations, les altérations ou les destructions et renforce l'environnement de contrôle d'ensemble afin de réduire les risques. Les cyberattaques peuvent avoir des conséquences directes et indirectes souvent importantes car les ordinateurs, les réseaux, les programmes, les données et les informations sensibles sont des éléments essentiels de la plupart des organisations. Étant donné que les organisations dépendent fortement des ressources informatiques, la direction devrait avoir pour priorité de définir clairement un plan de cybersécurité, des objectifs, des risques inhérents et des contrôles efficaces.

Cette Exigence Thématique fournit une approche cohérente et complète pour évaluer la conception et la mise en œuvre des processus de gouvernance, de gestion des risques et de contrôle en matière de cybersécurité.

GOUVERNANCE : Évaluer la gouvernance en matière de cybersécurité

Exigences :

Lors d'une mission d'audit interne incluant des objectifs liés à la cybersécurité dans son périmètre, les auditeurs internes doivent évaluer si les processus de gouvernance de l'organisation prennent en compte la cybersécurité de manière adéquate. Les auditeurs internes doivent évaluer si :

A. Des politiques et des procédures relatives aux processus de gestion des risques liés à la cybersécurité sont établies et périodiquement mises à jour, y compris la promotion de pratiques qui renforcent l'environnement de contrôle sur la base de cadres de référence largement adoptés (NIST, COBIT, et autres).

B. Les rôles et les responsabilités qui concourent à la réalisation des objectifs de l'organisation en matière de cybersécurité sont clairement définis et ces rôles sont assumés par des personnes possédant les connaissances, les compétences et les aptitudes requises.

C. Les mises à jour des objectifs, des stratégies, des risques et des contrôles d'atténuation en matière de cybersécurité sont périodiquement communiquées au Conseil.

D. Les parties prenantes concernées (par exemple, la direction, les opérations, les fournisseurs stratégiques et autres) sont invitées à discuter de la meilleure façon d'établir et d'améliorer les processus de gestion des risques liés à la cybersécurité.

E. Les ressources nécessaires (telles que le leadership, le financement, les talents, le matériel, les logiciels et la formation) pour exécuter efficacement les processus de gestion des risques de cybersécurité sont communiquées au Conseil.

GESTION DES RISQUES : Évaluer la gestion des risques liés à la cybersécurité

Exigences :

Lors d'une mission d'audit interne incluant des objectifs liés à la cybersécurité dans son périmètre, les auditeurs internes doivent évaluer si les processus de management des risques de l'organisation prennent en compte la cybersécurité de manière adéquate. Les auditeurs internes doivent évaluer si :

A. Un processus de gestion des risques à l'échelle de l'organisation est mis en place, qui comprend l'identification, l'analyse et la gestion des risques liés aux technologies de l'information et à la sécurité, en mettant l'accent sur les risques liés à la cybersécurité et sur la manière dont ces risques peuvent affecter la capacité à atteindre les objectifs de l'organisation.

B. Les processus de gestion des risques liés à la cybersécurité sont menés par une équipe plurifonctionnelle qui comprend la direction des technologies de l'information, la gestion des risques à l'échelle de l'organisation, la direction juridique, la direction de la conformité, d'autres directions (opérations, comptabilité, finances et autres) et associe, le cas échéant, les parties externes concernées (vendeurs, prestataires de services externalisés, fournisseurs, clients et autres).

C. Des politiques et des procédures de gestion du risque de cybersécurité ont été mises en place et sont périodiquement mises à jour, y compris la promotion de pratiques qui renforcent les processus de gestion du risque de cybersécurité sur la base de cadres de référence de gestion du risque largement adoptés, d'orientations faisant autorité ou d'autres meilleures pratiques.

D. L'obligation de rendre compte et la responsabilité de la gestion des risques liés à la cybersécurité sont établies et une personne ou une équipe a été désignée pour contrôler et communiquer périodiquement la manière dont les risques liés à la cybersécurité sont gérés, y compris les besoins en ressources pour atténuer les risques et l'identification des risques émergents liés à la cybersécurité qui n'avaient pas été recensés auparavant.

E. Un processus est mis en place pour faire remonter rapidement tout risque de cybersécurité (émergent ou déjà identifié) qui atteint un niveau inacceptable sur la base des lignes directrices établies par l'organisation en matière de gestion des risques ou pour se conformer aux exigences légales et/ou réglementaires applicables.

F. La gestion des risques liés à la cybersécurité comprend la coordination entre la sécurité de l'information, le service juridique, la conformité, entre autres fonctions, afin d'identifier et de respecter toutes les obligations légales et contractuelles, telles que les lois et les réglementations. Le statut de conformité et de non-conformité aux exigences applicables est communiqué périodiquement au sein de l'organisation.

G. Un processus est mis en place pour identifier et gérer les risques de cybersécurité liés aux tiers. Les fournisseurs et les prestataires de services externalisés sont contractuellement tenus de mettre en œuvre des contrôles de cybersécurité efficaces qui protègent de manière adéquate la confidentialité, l'intégrité et la disponibilité des systèmes et des données de l'organisation auxquels les tiers ont accès.

H. Des politiques et processus relatifs à la classification, à la conservation, à la destruction et au cryptage des données sont conçus de manière adéquate et déployés efficacement afin de fournir une approche systématique garantissant un enregistrement complet et précis des données et protégeant la confidentialité et le caractère privé des informations sensibles.

I. Un processus est établi pour communiquer les risques opérationnels liés à la cybersécurité afin que la direction et les employés en soient conscients. Les problèmes, lacunes, insuffisances ou défaillances de contrôle sont communiqués au Conseil et à la direction, et l'état d'avancement des mesures correctives leur est rapporté et fait l'objet d'un suivi étroit. Les cas de non-respect des politiques de cybersécurité sont identifiés, examinés, signalés et corrigés en temps utile.

CONTRÔLES : Évaluer les processus de contrôle de la cybersécurité

Exigences :

Lors d'une mission d'audit interne incluant des objectifs de cybersécurité dans son périmètre, les auditeurs internes doivent déterminer si les processus de contrôle de l'organisation prennent en compte la cybersécurité de manière adéquate. Les auditeurs internes doivent déterminer si l'organisation :

A. Priorise les contrôles de cybersécurité et veille à ce que le budget et les ressources correspondants (personnel, logiciels, outils, etc.) soient alloués de manière à maximiser les avantages escomptés.

B. Veille à ce que les contrôles de cybersécurité fonctionnent de manière à favoriser la réalisation des objectifs de l'organisation en matière de cybersécurité et la résolution rapide des problèmes.

C. Fournit une formation suffisante au personnel chargé des opérations de cybersécurité.

D. A élaboré des politiques et des procédures suffisantes pour gérer tous les aspects des opérations de cybersécurité et des contrôles sous-jacents.

E. Veille à ce que le management dispose des ressources nécessaires pour se tenir informée des problèmes de cybersécurité émergents liés aux nouvelles technologies, recenser les possibilités d'améliorer les opérations et comprendre comment les efforts en matière de cybersécurité peuvent être déployés au mieux pour contribuer aux buts et objectifs plus larges de l'organisation.

F. Intègre de manière adéquate la cybersécurité dans le cycle de développement des systèmes pour les applications d'entreprise, y compris les logiciels et les applications acquises ou développées sur mesure.

G. A inclus la cybersécurité dans la gestion du matériel (ordinateurs portables, ordinateurs de bureau, appareils mobiles).

H. A mis en œuvre des contrôles efficaces concernant le support du matériel de production, tels que la configuration, le déploiement des correctifs (patching), la gestion de l'accès des utilisateurs et le suivi de la disponibilité et des performances. L'organisation a évalué l'adéquation de la conception et l'efficacité opérationnelle de ces contrôles.

I. Optimise les contrôles liés au réseau en ce qui concerne la segmentation du réseau, l'utilisation et l'emplacement des pare-feu, les connexions limitées aux réseaux et/ou systèmes externes et l'utilisation de technologies de prévention et de détection telles que les systèmes de détection/prévention des intrusions (IDS/IPS).

J. A mis en œuvre des contrôles efficaces concernant les services de communication bureautique courants tels que le courrier électronique, les navigateurs Internet, la vidéoconférence, la messagerie et les protocoles de partage de fichiers.

K. A mis en œuvre des contrôles adéquats sur la fourniture de services afin de s'assurer que les domaines suivants sont intégrés dans la surveillance de la cybersécurité : gestion des changements, service de support et d'assistance (help desk) et administration des appareils des utilisateurs finaux.

L. A mis en place des contrôles de sécurité physique adéquats pour protéger les centres d'information à haut risque (tels que les centres de données, les centres d'exploitation de réseau et les centres opérationnels de sécurité - SOC) contre les attaques.

M. A mis en œuvre des contrôles de réponse aux incidents et de récupération.

Normes connexes :

3.1 Compétence
4.2 Conscience professionnelle
9.1 Compréhension les processus de gouvernance, de gestion des risques et de contrôle
9.4 Plan d'audit interne
12.3 Supervision et amélioration de la réalisation de la mission
13.1 Communication relative à la mission
13.2 Évaluation des risques dans le cadre de la mission
13.3 Objectifs et périmètre de la mission
13.4 Critères d'évaluation
13.5 Ressources de la mission
13.6 Programme de travail
14.1 Collecte d'informations pour analyses évaluation
14.2 Analyses et constats potentiels de la mission
14.3 Évaluation des constats
14.4 Recommandations et plans d'action
14.5 Conclusions de la mission
14.6 Documentation relative à la mission
15.1 Communication finale des résultats de la mission
15.2 Confirmation de la mise en œuvre des recommandations ou plans d'action

Guides pratiques d'audit des technologies de l'information (GTAG) connexes :

Évaluer le risque de cybersécurité : le modèle des trois lignes
Audit des applications
Audit de la réponse aux incidents cyber et de la récupération
Audit des opérations de cybersécurité : Prévention et détection
Audit de la gestion des identités et des accès
Audit de la gouvernance des systèmes d'information
Audit de l'informatique mobile
Audit de la gestion des réseaux et des télécommunications

Annexe A. Eléments à prendre en compte pour la mise en œuvre

Eléments à prendre en compte pour chaque exigence liée à la gouvernance :

Pour évaluer la manière dont les processus essentiels de gouvernance sont appliqués aux objectifs de cybersécurité, les auditeurs internes peuvent examiner les éléments suivants :

A. Politiques, procédures et autres documents pertinents utilisés par l'organisation pour gérer les responsabilités courantes en matière de cybersécurité, notamment :
   1. Une documentation claire, concise, cohérente et mise à jour périodiquement, idéalement au fur et à mesure de l'identification des nouveaux risques de cybersécurité et au moins une fois par an.
   2. Procédures relatives à l'identification, à l'analyse, à la résolution et au signalement des violations ou autres pertes de données sensibles.
   3. Documentation sur la manière dont la direction s'assure que les politiques et les procédures sont suffisantes pour soutenir les opérations de cybersécurité.

B. Rôles et responsabilités définis par le Conseil pour soutenir la réalisation de la stratégie de cybersécurité, y compris un positionnement organisationnel qui garantit que la cybersécurité relève d'un niveau de l'organisation disposant d'une visibilité suffisante pour soutenir l'organisation.

C. Les documents présentés au Conseil concernant la stratégie, les objectifs, les risques et les contrôles en matière de cybersécurité, y compris en déterminant si :
   1. La fréquence de communication est adéquate, idéalement trimestrielle et présentée par un responsable de la fonction sécurité de l'information, tel que le directeur des systèmes d'information.
   2. Les informations présentées sont claires, concises et cohérentes ; les risques et les contrôles sont communiqués de manière à être facilement compris par le Conseil.
   3. Les indicateurs clés de performance ou d'autres mesures/statistiques importantes en matière de cybersécurité sont inclus.
   4. Le cas échéant, les commentaires du Conseil sont reçus par la direction et mis en œuvre, et des mises à jour sur l'état d'avancement des changements sont communiquées au Conseil.

D. Preuve de la communication de la direction en charge de la cybersécurité avec les parties prenantes concernées (par exemple, la direction, les opérations, les fournisseurs stratégiques et autres), y compris le fait que les informations communiquées sont claires, concises, cohérentes et adaptées à l'audience des parties prenantes :
   1. Les employés.
   2. Les vendeurs, les fournisseurs, les prestataires de services externalisés et les tiers.
   3. Les clients.
   4. Partenaires stratégiques.

E. L'analyse et la communication des besoins en ressources par la direction, y compris :
   1. Comprendre comment les lacunes sont identifiées et quelles indicateurs clés sont utilisées pour anticiper les changements dans les exigences.
   2. Comment la direction collabore avec les ressources humaines pour analyser les besoins en talents dans le domaine de la cybersécurité.
   3. Comment la direction analyse les inventaires actuels de matériels et de logiciels et détermine si des investissements supplémentaires sont nécessaires pour soutenir les initiatives en matière de cybersécurité.
   4. Si les auditeurs internes examinent la manière dont la direction établit et met à jour les supports de formation à la cybersécurité et identifie les lacunes, notamment en veillant à ce que la formation couvre les nouveaux objectifs, risques et contrôles en matière de cybersécurité.

Eléments à prendre en compte pour chaque exigence en matière de gestion des risques :

Pour évaluer les aspects requis de la gestion du risque de cybersécurité, les auditeurs internes peuvent examiner les éléments suivants :

A. Comment la direction identifie-t-elle initialement les risques de cybersécurité ?
    1. Comprendre quel personnel est responsable des menaces courantes auxquelles l'organisation est confrontée et des risques émergents avec la communauté de la sécurité de l'information.
        a. Determiner si ces personnes ont l'expérience professionnelle et la formation requises pour reconnaître efficacement les menaces et les transmettre à l'équipe de gestion des risques au sens large.
    2. Identifier les solutions logicielles ou les fournisseurs sur lesquels la direction s'appuie pour identifier les risques de cybersécurité.
    3. Documentation relative au processus de gestion des risques en matière de cybersécurité, y compris :
        a. Procès-verbal de réunions.
        b. Plan d'actions à mettre en œuvre. .
        c. Listes des participants ou des membres de l'équipe.
        d. Enquête post-incident/analyse des causes racines.

B. La manière dont la direction identifie ou désigne les membres de l'équipe de gestion des risques, ainsi que le raisonnement ou les qualifications utilisés pour évaluer la composition de l'équipe. Examiner les preuves de de discussions périodiques sur les risques liés à la cybersécurité avec les parties externes concernées.

C. Le processus utilisé par l'organisation pour établir et mettre à jour périodiquement les politiques et procédures relatives à la gestion du risque de cybersécurité, qui peut inclure :
    1. Une révision et une approbation annuelles des politiques et des procédures.
    2. Une compréhension de la manière dont l'organisation assure le respect de ses politiques et procédures de gestion des risques et de la manière dont le personnel est formé à l'exécution des politiques et procédures.
        a. Une compréhension des cadres de référence ou des orientations faisant autorité que la direction utilise pour gérer les risques de cybersécurité (NIST, COBIT et autres) et de la manière dont l'organisation confirme l'adhésion au(x) cadre(s) de référence choisi(s).

D. La ou les personnes chargées de mettre en œuvre la gestion des risques liés à la cybersécurité, notamment en s'assurant que leur parcours professionnel, leur expérience, leurs qualifications et leurs compétences sont adaptés à la gestion des risques et des menaces liés à la sécurité de l'information. Vérifier que la personne responsable est positionnée à un niveau de l'organisation qui lui permet de donner de la visibilité aux risques de cybersécurité et de communiquer efficacement sur ces risques.

E. Les processus de remontée des informations que l'organisation utilise pour communiquer sur les risques de cybersécurité, y compris la manière dont le niveau de menace ou de risque est évalué, affecté et priorisé. Vérifier que l'organisation a défini des niveaux de risque (comme par exemple élevé, modéré, faible), y compris une explication détaillée de chaque niveau de risque et des procédures d'escalade pour chaque catégorie de risque. Examiner la liste des risques de cybersécurité actuellement recensés et l'état d'avancement des mesures d'atténuation pour chaque événement.

F. Le processus utilisé par l'organisation pour veiller à la conformité avec toutes les réglementations applicables en matière de cybersécurité, y compris :
    1. L'impact des réglementations proposées ou récemment adoptées sur l'organisation.
    2. S'il existe un inventaire des réglementations applicables qui fait l'objet d'un suivi, d'une mise à jour et d'un rapport périodique afin de garantir la sensibilisation de l'organisation.

a. Pour tout élément de non-conformité, vérifier que la direction est consciente des risques associés, notamment par le biais de rapports périodiques.

G. Le processus de gestion des risques de cybersécurité liés aux tiers mis en place par l'organisation. Vérifier que les contrôles de cybersécurité des fournisseurs sont examinés avant le début de la relation commerciale et que les contrats prévoient le droit à des examens périodiques tout au long de la relation. Il s'agit notamment d'obtenir et d'analyser le rapport sur les contrôles de l'organisation de services du tiers et de vérifier que l'organisation a documenté l'examen de son rapport SOC, ce qui devrait permettre de s'assurer que les considérations relatives au contrôle de l'utilisateur ont été mises en œuvre. Comprendre l'approche adoptée par la direction pour déterminer si les tiers disposent d'un environnement de contrôle adapté aux contrôles de l'organisation.
   a. Si des faiblesses sont constatées dans les contrôles des tiers, il convient de comprendre le processus utilisé par la direction pour s'assurer que ces faiblesses ne compromettent pas la cybersécurité des opérations, ou de comprendre comment l'organisation fait savoir que des changements sont nécessaires pour maintenir la relation avec le fournisseur concerné ou qu'il convient éventuellement de trouver un fournisseur de remplacement.

H. Les politiques et les processus mis en place par l'organisation en ce qui concerne :
   1. La classification des données.
   2. La conservation des données.
   3. La destruction des données.
   4. Le chiffrement.
   5. La gestion des accès et des identités.
   6. Qui prépare, révise et met à jour la documentation, ce qui devrait idéalement impliquer le personnel juridique et conformité afin de veiller à la conformité avec les réglementations applicables.
   7. La manière dont l'organisation procède à la classification des données pour s'assurer que les données confidentielles et privées ont été identifiées et qu'elles bénéficient du niveau de protection approprié, par exemple en limitant l'accès des utilisateurs.
   8. Comment l'organisation examine-t-elle périodiquement le processus mis en œuvre pour classer les données et si ce processus soutient les objectifs de cybersécurité de l'organisation et est conforme aux politiques de l'organisation et aux réglementations applicables.

I. Le processus de communication des risques opérationnels liés à la cybersécurité à la direction et aux employés. Idéalement, cette communication devrait être incluse dans une formation périodique à la cybersécurité (au moins une fois par an). Comprendre la procédure suivie par la direction pour communiquer des mises à jour sur les mesures correctives prises pour remédier aux problèmes de cybersécurité, ainsi que les dates d'achèvement prévues. Vérifier que les cas de non-conformité font l'objet d'un suivi attentif et que des mises à jour sont communiquées au Conseil et à la direction.

Eléments à prendre en compte pour chaque exigence du processus de contrôle :

Pour évaluer les aspects requis des contrôles de cybersécurité, les auditeurs internes peuvent examiner les éléments suivants :

A. Le processus suivi par la direction pour déterminer comment déployer les ressources budgétisées à l'appui de l'environnement de contrôle de la cybersécurité, ce qui devrait comprendre une planification stratégique annuelle visant à assurer qu'un niveau adapté de ressources est disponible pour atteindre les objectifs en matière de cybersécurité. Les résultats formels et documentés de la planification annuelle et du suivi périodique de la gestion des ressources devraient être examinés.

B. Le processus mis en place par la direction pour évaluer périodiquement que les contrôles de cybersécurité fonctionnent de manière à favoriser la réalisation des objectifs de l'organisation en matière de cybersécurité. Vérifier que la direction surveille l'efficacité des contrôles et évalue si les contrôles existants sont conçus de manière appropriée ou si de nouveaux contrôles sont nécessaires. Dans de nombreuses organisations, la fonction d'audit interne joue un rôle important dans ce processus en fournissant une assurance sur la conception des contrôles et sur l'efficacité de leur fonctionnement au moyen de tests périodiques (trimestriels ou annuels). Vérifier les processus mis en place par la direction pour remédier aux déficiences des contrôles ou pour traiter les résultats des évaluations réalisées par la fonction d'audit interne ou par d'autres prestataires d'assurance (par exemple, les tests de pénétration).

C. Le processus suivi par la direction pour évaluer les besoins de formation du personnel chargé de la cybersécurité au sein de l'organisation et la manière dont les ressources sont affectées pour dispenser une formation appropriée et faire en sorte que les nouvelles menaces en matière de cybersécurité soient comprises et gérées. Comprendre comment la direction s'assure que les employés disposent de formations suffisante en matière de cybersécurité, ce qui peut inclure des formations en direct ou enregistrées ou la réalisation de modules de formation (autoformation, e-learning, etc.).

D. Le processus mis en place par l'organisation pour définir et mettre à jour les politiques et procédures en matière de cybersécurité et la manière dont la direction évalue l'adéquation de ces politiques et procédures. Comprendre comment le personnel responsable des opérations et des contrôles en matière de cybersécurité est formé au respect des politiques et des procédures et comment cette conformité est évaluée.

E. Le processus mis en place par l'organisation pour former de manière appropriée l'équipe de direction responsable des opérations et des contrôles en matière de cybersécurité afin qu'elle reconnaisse les tendances émergentes et qu'elle fournisse à ses équipes et à l'organisation un leadership stratégique. Comprendre comment l'organisation identifie les possibilités d'accroître les capacités de l'encadrement pour favoriser la prise de conscience des problèmes émergents, par exemple en participant à des programmes de formation professionnelle continue.

F. La manière dont l'organisation gère la cybersécurité dans le cadre du cycle de vie du développement des systèmes, y compris les aspects de contrôle suivants :
    1. La planification : La cybersécurité a été identifiée comme un élément clé de l'évaluation des risques et de l'analyse des vulnérabilités potentielles. La portée et les objectifs de la mise en œuvre des logiciels doivent être pris en compte lorsque l'organisation évalue les contrôles de cybersécurité au cours de la phase de planification.
    2. Le recueil des exigences : Les exigences en matière de cybersécurité sont une composante de la définition des exigences fonctionnelles, définition qui doit également inclure le respect de toutes les exigences légales et réglementaires applicables.
    3. La conception : Les considérations relatives à la cybersécurité font partie intégrante des exigences de traitement détaillées. Les contrôles doivent être identifiés dans tous les aspects de la conception au fur et à mesure que l'organisation définit plus formellement les besoins de la conception de l'architecture du système (tels que les plates-formes, les interfaces utilisateur, les bases de données et autres).
    4. Le développement : L'organisation a mis en place un environnement sécurisé et défini formellement un processus de développement qui minimise les vulnérabilités cyber (par exemple, un accès limité des utilisateurs au code de développement, une séparation appropriée de l'environnement de production, l'utilisation d'outils approuvés, l'existence de pistes d'audit pour suivre les activités de développement, des exigences de cybersécurité spécifiques pour les logiciels développés par les fournisseurs, et autres).
    5. Les tests : L'organisation inclut l'examen et l'évaluation de la cybersécurité dans la phase de test (par exemple, tests automatisés, tests de pénétration et évaluation des vulnérabilités). L'organisation doit être en mesure d'être rapidement alertée de toute vulnérabilité cyber identifiée lors des tests et d'y remédier, ce qui inclut

une description détaillée de la vulnérabilité et des modifications de code ou des contrôles d'atténuation mis en place en réponse à cette vulnérabilité.

6. Le déploiement : Lors de la mise en production d'un nouveau logiciel, l'organisation doit surveiller attentivement les menaces potentielles pour la cybersécurité, notamment en s'assurant que les utilisateurs finaux ont été formés à l'utilisation du logiciel d'une manière qui minimise les risques pour la cybersécurité. L'organisation doit veiller à ce que les événements et les erreurs soient consignés et analysés en relation avec les événements potentiels de cybersécurité.
7. La maintenance : L'organisation devrait veiller à ce que toutes les versions des logiciels liés à la sécurité soient appliquées en temps utile et devrait avoir une communication ouverte avec les fournisseurs de logiciels pour s'assurer que les risques et menaces émergents sont correctement contrôlés et que les utilisateurs finaux sont informés de toutes les vulnérabilités connues.

G. Contrôles mis en place par l'organisation pour protéger le matériel (ordinateurs de bureau, ordinateurs portables, appareils mobiles et autres) contre les risques de cybersécurité, ce qui inclut l'utilisation du cryptage, de logiciels antivirus, de mots de passe complexes, de réseaux privés virtuels (VPN) ou de réseaux zéro confiance (zero-trust network) pour l'authentification, la mise à jour périodique des microprogrammes et un processus de gestion des actifs qui garantit que le matériel fourni par l'entreprise dispose d'une configuration de sécurité appropriée au moment de sa mise à disposition et qu'il est correctement mis hors service lorsque ce matériel est décommissionné.

H. Les contrôles que l'organisation a mis en place pour garantir que les services de production informatique offre une protection contre les risques de cybersécurité, ce qui devrait inclure le fait que les serveurs sont corrigés (patchés) avec des versions de sécurité en temps opportun afin d'atténuer les risques émergents. Examiner les contrôles de surveillance mis en place pour déterminer si la disponibilité et l'utilisation des ressources sont satisfaisantes, ce qui permet d'examiner et d'analyser les éventuels problèmes de cybersécurité qui menacent les performances. Examiner les contrôles liés aux bases de données, notamment la limitation de l'accès des utilisateurs et des administrateurs, l'utilisation du cryptage, la sauvegarde et le test de restauration des bases de données, ainsi que la présence de contrôles robustes de sécurité sur le réseau.

I. Contrôles liés au réseau qui prévoient une segmentation afin de limiter les risques de cybersécurité liés à un accès non autorisé. Examiner la manière dont l'organisation utilise les pare-feu, y compris leur emplacement et le processus utilisé pour examiner, analyser et restreindre l'accès au réseau, afin d'empêcher les accès non autorisés. Examiner comment l'organisation utilise les systèmes de détection/prévention des intrusions (IDS/IPS) pour prévenir et détecter les attaques de cybersécurité et y remédier.

J. Contrôles mis en place par l'organisation autour des services bureautiques courants de communication, tels que l'utilisation du cryptage du courrier électronique, la garantie que les mises à jour de sécurité du navigateur internet sont appliquées en temps opportun, la configuration des paramètres de sécurité de la vidéoconférence/messagerie (par exemple, MS Teams, Zoom et autres) pour restreindre l'utilisation de certaines extensions de fichiers (telles que les fichiers .exe), et l'utilisation de l'authentification multi facteur pour le partage de fichiers.

K. Les contrôles que l'organisation a mis en place pour atténuer les risques de cybersécurité liés à la fourniture de services, notamment :

1. Veiller à ce que le processus de gestion des changements prenne en compte les risques de cybersécurité lors de l'évaluation et de l'approbation des changements, et à ce que la réponse aux incidents cyber se fasse en temps opportun.
2. Le service d'assistance aux utilisateurs enregistre tous les événements de cybersécurité communiqués par l'organisation, veille à ce qu'ils soient résolus en temps opportun et les transmet au membre de la direction concerné.

3. L'administration des appareils mobiles (comme le courrier électronique, les applications et autres) est configurée pour atténuer les risques de cybersécurité et peut être gérée à distance si l'appareil d'un utilisateur est compromis.

L. Les contrôles de sécurité physique visant à protéger les informations à haut risque, y compris contre les risques de cybersécurité. Il s'agit par exemple de s'assurer que l'accès des tiers/fournisseurs est approprié et de limiter l'accès physique des utilisateurs aux centres de données, aux centres d'exploitation des réseaux et aux centres opérationnels de sécurité (SOC) au personnel autorisé.

M. Les contrôles mis en œuvre par l'organisation en ce qui concerne la réponse aux incidents et la récupération, notamment :
   1. Un plan documenté qui est revu et mis à jour au fur et à mesure de l'évolution des activités de l'organisation.
   2. Des tests périodiques et la communication des résultats à la direction.
   3. L’identification et la résolution en temps opportun des problèmes mis en évidence par ces tests.

Annexe B. Outil pour documenter la conformité à une Exigence Thématique

Cybersécurité - Gouvernance

Exigence	Conformité (Oui / Non / Partielle)	Preuves obtenues ou justification de l'exclusion
A. Des politiques et des procédures relatives aux processus de gestion des risques liés à la cybersécurité sont établies et périodiquement mises à jour, y compris la promotion de pratiques qui renforcent l'environnement de contrôle sur la base de cadres de référence largement adoptés (NIST, COBIT, et autres).		
B. Les rôles et les responsabilités qui concourent à la réalisation des objectifs de l'organisation en matière de cybersécurité sont clairement définis et ces rôles sont assumés par des personnes possédant les connaissances, les compétences et les aptitudes requises.		
C. Les mises à jour des objectifs, des stratégies, des risques et des contrôles d'atténuation en matière de cybersécurité sont communiquées périodiquement au Conseil.		
D. Les parties prenantes concernées (par exemple, la direction, les opérations, les fournisseurs stratégiques et autres) sont invitées à discuter de la meilleure façon d'établir et d'améliorer les processus de gestion des risques liés à la cybersécurité.		
E. Les ressources nécessaires (telles que le leadership, le financement, les talents, le matériel, les logiciels, et la formation) pour exécuter efficacement les processus de gestion des risques liés à la cybersécurité sont communiquées au Conseil.		

Cybersécurité - Gestion des risques

Exigence	Conformité (Oui / Non / Partielle)	Preuves obtenues ou justification de l'exclusion
A. Un processus de gestion des risques à l'échelle de l'organisation est mis en place, qui comprend l'identification, l'analyse et la gestion des risques liés aux technologies de l'information et à la sécurité, en mettant l'accent sur les risques liés à la cybersécurité et sur la manière dont ces risques peuvent		

Exigence	Conformité (Oui / Non / Partielle)	Preuves obtenues ou justification de l'exclusion
affecter la capacité à atteindre les objectifs de l'organisation.		
B. Les processus de gestion des risques liés à la cybersécurité sont menés par une équipe plurifonctionnelle qui comprend la direction des technologies de l'information, la gestion des risques à l'échelle de l'organisation, la direction juridique, la direction de la conformité et d'autres directions (par exemple, la direction des opérations, la direction comptable/financière) et associe, le cas échéant, les parties externes concernées (vendeurs, fournisseurs, clients et autres).		
C. Des politiques et des procédures relatives à la gestion du risque de cybersécurité ont été établies et sont périodiquement mises à jour, y compris la promotion de pratiques qui renforcent les processus de gestion du risque de cybersécurité sur la base de cadres de référence de gestion du risque largement adoptés, d'orientations faisant autorité ou de meilleures pratiques.		
D. L'obligation de rendre compte et la responsabilité de la gestion des risques liés à la cybersécurité sont établies et une personne ou une équipe a été désignée pour contrôler et communiquer périodiquement la manière dont les risques liés à la cybersécurité sont gérés, y compris les besoins en ressources pour atténuer les risques et l'identification des risques émergents liés à la cybersécurité qui n'avaient pas été recensés auparavant.		
E. Un processus est mis en place pour faire remonter rapidement les risques de cybersécurité (émergents ou déjà identifiés) qui atteignent des niveaux inacceptables sur la base des lignes directrices établies par l'organisation en matière de gestion des risques ou pour se conformer aux exigences légales et/ou réglementaires applicables.		
F. La gestion des risques liés à la cybersécurité comprend la coordination entre la sécurité de l'information, le service juridique, le service de la conformité et d'autres services de gestion afin d'identifier et de respecter toutes les obligations légales et contractuelles (lois, règlements). L'état de la conformité et de la non-conformité aux exigences applicables est communiqué périodiquement à l'organisation.		

Exigence	Conformité (Oui / Non / Partielle)	Preuves obtenues ou justification de l'exclusion
G. Un processus est en place pour identifier et gérer les risques de cybersécurité liés aux tiers. Les vendeurs, les fournisseurs et les autres prestataires de processus et/ou de services externalisés sont contractuellement tenus de mettre en œuvre des contrôles de cybersécurité efficaces qui protègent de manière adéquate la confidentialité, l'intégrité et la disponibilité des systèmes et des données de l'organisation auxquels ils ont accès.		
H. Des politiques et processus relatifs à la classification, à la conservation, à la destruction et au cryptage des données sont conçus de manière adéquate et déployés efficacement afin de fournir une approche systématique garantissant un enregistrement complet et précis des données et protégeant la confidentialité et le caractère privé des informations sensibles.		
I. Un processus est en place pour communiquer les risques opérationnels liés à la cybersécurité afin de garantir une sensibilisation adéquate de la direction et des employés. Les problèmes, les lacunes, les insuffisances et les défaillances des contrôles sont communiqués au Conseil et à la direction, et l'état d'avancement des mesures correctives leur est rapporté et fait l'objet d'un suivi étroit. Les cas de non-respect des politiques de cybersécurité sont identifiés, examinés, signalés et corrigés en temps utile.		

Cybersécurité - Processus de contrôle

Exigence	Conformité (Oui / Non / Partielle)	Preuves obtenues ou justification de l'exclusion
A. Priorise les contrôles de cybersécurité et veille à ce que le budget et les ressources correspondants (personnel, logiciels, outils, etc.) soient alloués de manière à maximiser les avantages escomptés.		
B. Veille à ce que les contrôles de cybersécurité fonctionnent de manière à favoriser la réalisation des objectifs de l'organisation en matière de cybersécurité et la résolution rapide des problèmes.		

Exigence	Conformité (Oui / Non / Partielle)	Preuves obtenues ou justification de l'exclusion
C. Fournit une formation suffisante au personnel chargé des opérations de cybersécurité.		
D. A élaboré des politiques et des procédures suffisantes pour gérer tous les aspects des opérations de cybersécurité et des contrôles sous-jacents.		
E. Veille à ce que la direction dispose des ressources nécessaires pour se tenir informée des problèmes de cybersécurité émergents liés aux nouvelles technologies, recenser les possibilités d'améliorer les opérations et comprendre comment les efforts en matière de cybersécurité peuvent être déployés au mieux pour avoir une incidence sur les buts et objectifs plus larges de l'organisation.		
F. Intègre de manière adéquate la cybersécurité dans le cycle de développement des systèmes pour les applications d'entreprise, y compris les logiciels et les applications acquises ou développées sur mesure.		
G. A inclus la cybersécurité dans la gestion du matériel (ordinateurs portables, ordinateurs de bureau, appareils mobiles).		
H. A mis en œuvre des contrôles efficaces concernant le support du matériel de production, tels que la configuration, le déploiement de correctifs (patching), la gestion de l'accès des utilisateurs et le suivi de la disponibilité et des performances. L'organisation a évalué l'adéquation de la conception et l'efficacité opérationnelle de ces contrôles.		
I. Optimise les contrôles liés au réseau en ce qui concerne la segmentation du réseau, l'utilisation et l'emplacement des pare-feu, les connexions limitées aux réseaux et/ou systèmes externes et l'utilisation de technologies de prévention et de détection telles que les systèmes de détection/prévention des intrusions (IDS/IPS).		
J. A mis en œuvre des contrôles efficaces concernant les services de communication bureautique courants tels que le courrier électronique, les navigateurs Internet, la		

Exigence	Conformité (Oui / Non / Partielle)	Preuves obtenues ou justification de l'exclusion
vidéoconférence, la messagerie et les protocoles de partage de fichiers.		
K. A mis en œuvre des contrôles adéquates de la fourniture de services pour s'assurer que les domaines suivants sont intégrés dans la surveillance de la cybersécurité : gestion des changements, service de support et d'assistance (help desk) et administration des appareils des utilisateurs finaux.		
L. A mis en œuvre des contrôles de sécurité physique adéquate pour protéger les centres d'information à haut risque (tels que les centres de données – data centers, les centres d'exploitation de réseau et les centres opérationnels de sécurité - SOC) contre les attaques.		
M. A mis en œuvre des contrôles de réponse aux incidents et de récupération.		

À propos de l'Institut des auditeurs internes

L'Institut des auditeurs internes (IIA) est une association professionnelle qui compte plus de 245 000 membres dans le monde et a délivré plus de 195 000 certifications d'auditeur interne (CIA) dans le monde entier. Fondé en 1941, l'IIA est reconnu dans le monde entier comme le leader de la profession d'audit interne en matière de normes, de certifications, d'éducation, de recherche et de conseils techniques. Pour plus d'informations, visitez le site www.theiia.org.

Clause de non-responsabilité

L'IIA publie ce document à des fins d'information et d'éducation. Ce document n'est pas destiné à fournir des réponses définitives à des situations individuelles spécifiques et, en tant que tel, il est uniquement destiné à être utilisé comme un guide. L'IIA recommande de demander l'avis d'un expert indépendant pour toute situation spécifique. L'IIA décline toute responsabilité à l'égard des personnes qui s'appuient exclusivement sur ce document.

Droit d'auteur

avril 2024

The Institute of
Internal Auditors

Siège mondial
Institut des auditeurs internes
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746, USA
Téléphone : +1-407-937-1111
Fax : +1-407-937-1101