# Cybersécurité

## *Topical Requirement*

## *Exigence Thématique*

## *Guide de l'utilisateur*

The Institute of
**Internal Auditors**

# Contenu

# Aperçu des exigences thématiques

Les exigences thématiques sont une composante essentielle du Cadre International des Pratiques Professionnelles (International Professional Practices Framework®), au même titre que les Normes Internationales d'audit interne (Global Internal Audit Standards™) et les Lignes directrices internationales. L'Institut des auditeurs internes requiert que les Exigences Thématiques soient utilisées conjointement avec les Normes internationales de l'audit interne, qui constituent la référence faisant autorité des pratiques requises. Des références aux Normes apparaissent tout au long de ce guide comme source d'informations plus détaillées.

Les Exigences Thématiques formalisent la manière dont les auditeurs internes traitent les domaines de risques très courants afin de promouvoir la qualité et la cohérence au sein de la profession. Les Exigences Thématiques établissent une base de référence et fournissent des critères pertinents pour la réalisation de prestations d'assurance liées à l'objet d'une Exigence Thématique (Norme 13.4 Critères d'évaluation). La conformité aux Exigences Thématiques est obligatoire pour les services d'assurance et recommandée pour les services de conseil. Les Exigences Thématiques ne sont pas destinées à couvrir tous les aspects potentiels à prendre en compte lors des missions d'assurance ; elles sont plutôt destinées à fournir un ensemble minimum d'exigences permettant une évaluation cohérente et fiable du sujet.

Les Exigences Thématiques sont clairement liées au Modèle des Trois Lignes de l'IIA et aux normes internationales de l'audit interne. Les processus de gouvernance, de gestion des risques et de contrôle sont les principales composantes des Exigences Thématiques qui s'alignent sur la ”Norme 9.1 Compréhension des processus de gouvernance, de gestion des risques et de contrôle”. En référence au Modèle des Trois Lignes, la gouvernance est liée au Conseil ou à l'organe de direction, la gestion des risques est liée à la deuxième ligne, et les contrôles ou processus de contrôle sont liés à la première ligne. Alors que le management est représenté sur les deux premières lignes, la fonction d'audit interne est représentée sur la troisième ligne en tant que fournisseur d'assurance indépendant et objectif, rendant compte au Conseil/à l'organe de direction (principe 8 Surveillance du Conseil).

## Applicabilité, risque et jugement professionnel

Les Exigences Thématiques doivent être respectées lorsque les fonctions d'audit interne réalisent des missions d'assurance sur des sujets pour lesquels il existe une Exigence Thématique ou lorsque des aspects de l'Exigence Thématique sont identifiés dans le cadre d'autres missions d'assurance.

Comme le décrivent les Normes, l'évaluation des risques est un élément important de la planification par le responsable de l'audit interne. Pour déterminer les missions d'assurance à inclure dans le plan d'audit interne, il est nécessaire d'évaluer les stratégies, les objectifs et les risques de l'organisation au moins une fois par an (Norme 9.4 Plan d'audit interne). Lors de la planification de chaque mission d'assurance, les auditeurs internes doivent évaluer les risques liés à la mission (Norme 13.2 Évaluation des risques dans le cadre de la mission).

Lorsque le sujet d'une Exigence Thématique est identifié au cours du processus de planification de l'audit interne fondé sur les risques et qu'il est inclus dans le plan d'audit, les exigences décrites dans l'Exigence Thématique doivent être utilisées pour évaluer le sujet dans le cadre des missions concernées. En outre, lorsque les auditeurs internes réalisent une mission (qu'elle soit incluse ou non dans le plan) et que des éléments d'une Exigence Thématique apparaissent, l'applicabilité de cette exigence doit être évaluée dans le cadre de la mission. Enfin, si une mission est demandée alors qu'elle ne figurait pas initialement dans le plan et qu'elle porte sur le sujet en question, l'applicabilité de l'Exigence Thématique doit être évaluée.

Le jugement professionnel joue un rôle clé dans l'application de l'Exigence Thématique. L'évaluation des risques guide les décisions des responsables de l'audit interne quant aux missions à inclure dans le plan d'audit interne (Norme 9.4 Plan d'audit interne). En outre, les auditeurs internes font preuve de jugement professionnel pour déterminer les aspects à couvrir dans le cadre de chaque mission (Normes 13.3 Objectifs et périmètre de la mission, 13.4 Critères d'évaluation et 13.6 Programme de travail). L'annexe A, intitulée "Exemples d'application pratique", décrit comment les auditeurs internes déterminent si l'Exigence Thématique s'applique.

La preuve que l’applicabilité de chaque exigence de l'exigence thématique a été évaluée doit être conservée. Les exclusions d’une exigence de l’Exigence Thématique doivent être justifiées. La conformité à l'Exigence Thématique doit être documentée en utilisant le jugement professionnel de l'auditeur tel que décrit dans la norme “14.6 Documentation relative à la mission”.

Bien que l'Exigence Thématique relative à la cybersécurité fournisse une base de processus de contrôle à prendre en considération, les organisations qui évaluent le risque cyber comme étant très élevé peuvent avoir besoin d'évaluer des aspects supplémentaires.

Si le responsable de l'audit interne estime que la fonction d'audit interne ne possède pas les connaissances requises pour réaliser des missions d'audit sur un sujet relevant d'une Exigence Thématique, la mission peut être externalisée (Normes 3.1 Compétence, 7.2 Qualifications du responsable de l'audit interne, 10.2 Gestion des ressources humaines). Même dans ce cas, l'externalisation ne libère pas la fonction d'audit interne de sa responsabilité de se conformer aux Exigences Thématiques. Le responsable de l'audit interne conserve la responsabilité ultime d'assurer cette conformité. En outre, si le responsable de l'audit interne estime que les ressources de l'audit interne sont insuffisantes, il doit informer le Conseil de l'impact de cette insuffisance de ressources et de la manière dont elle sera comblée (norme 8.2 Ressources).

### *Performance, documentation et rapports*

Lorsqu'ils appliquent les exigences thématiques, les auditeurs internes doivent également se conformer aux Normes, en menant leurs travaux conformément au “Domaine V : Réalisation des activités d'audit interne”. Les Normes du domaine V décrivent la planification des missions (principe 13 : Planifier les missions avec efficacité), la réalisation des missions (principe 14 : Réaliser les travaux de la mission) et la communication des résultats de la mission (principe 15 : Communiquer les résultats de la mission et suivre les plans d'action).

La couverture de l'Exigence Thématique peut être documentée soit dans le plan d'audit interne, soit dans les documents de travail de la mission, sur la base du jugement professionnel des auditeurs. Une ou plusieurs missions d'audit interne peuvent couvrir les exigences. En outre, toutes les exigences peuvent ne pas être applicables. La preuve de l'évaluation de l'applicabilité de l'exigence thématique doit être conservée, y compris une justification des exclusions.

L'outil facultatif figurant à l'annexe C peut être utilisé comme référence et pour documenter le travail effectué par les auditeurs internes.

### *Assurance qualité*

Les Normes exigent du responsable de l'audit interne qu'il élabore, mette en œuvre et tienne à jour un programme d'assurance et d'amélioration qualité couvrant tous les aspects de la fonction d'audit interne (Norme 8.3 Qualité). Les résultats doivent être communiqués au Conseil et à la direction générale. Les communications doivent rendre compte de la conformité de la fonction d'audit interne avec les Normes et de la réalisation des objectifs de performance.

La conformité aux Exigences Thématiques sera évaluée dans le cadre des évaluations de la qualité. Pour préparer un examen de la qualité, les auditeurs internes peuvent utiliser l'outil figurant à l'annexe C.

### *Cybersécurité*

La cybersécurité est un vaste sujet lié à la plupart des aspects technologiques de toute organisation. Outre les technologies de l'information, la cybersécurité fait généralement partie des processus opérationnels, ce qui oblige les auditeurs internes à évaluer les risques cyber lors de la planification, du cadrage et de la réalisation des missions d'assurance.

Le National Institute of Standards and Technology (NIST), qui fait partie du ministère américain du commerce, définit la cybersécurité comme "la capacité à protéger ou à défendre l'utilisation du cyberespace contre les cyberattaques". L'Exigence Thématique relative à la cybersécurité se concentre sur le périmètre externe que les organisations sécurisent pour atténuer les risques liés aux utilisateurs non autorisés et aux cybermenaces malveillantes. La cybersécurité est un sous-ensemble de la sécurité globale de l'information, que le NIST définit comme "la protection des informations et des systèmes d'information contre l'accès, l'utilisation, la divulgation, la perturbation, la modification ou la destruction non autorisés, afin d'assurer la confidentialité, l'intégrité et la disponibilité".

Les exigences de l'Exigence Thématique relative à la cybersécurité sont les suivantes :

- Gouvernance - objectifs et stratégies clairement définis en matière de cybersécurité qui soutiennent les objectifs, les politiques et les procédures de l'organisation.
- Gestion des risques - processus d'identification, d'analyse, de gestion et de suivi des cybermenaces, y compris un processus de remontée rapide des risques cyber.

Contrôles - processus de contrôle établis par la direction et évalués périodiquement pour atténuer le risque cyber.

## Considérations

Les auditeurs internes peuvent s'appuyer sur les considérations suivantes pour faciliter leur évaluation des exigences de l'Exigence Thématique relative à la cybersécurité. Ces considérations, qui renvoient aux exigences, sont données à titre d'exemple mais ne sont pas obligatoires. Les auditeurs internes doivent s'appuyer sur leur jugement professionnel pour déterminer les éléments à inclure dans leur évaluation.

### *Considérations relatives à la gouvernance*

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

A. Un plan stratégique et des objectifs de cybersécurité formalisés et documentés, y compris la preuve que le Conseil examine périodiquement (généralement tous les trimestres) les mises à jour en matière de cybersécurité fournies par le responsable de la sécurité de l'information, tel que le chef de la sécurité de l'information (CISO). Les éléments probants peuvent inclure des rapports sur :
   - Le suivi de la réalisation des objectifs stratégiques.
   - Les besoins budgétaires pour soutenir les objectifs en matière de cybersécurité.
   - Les risques et les contrôles internes, y compris les progrès réalisés en matière de remédiation.
   - Les indicateurs clés de performance (KPI) pour mesurer les succès.

Les ressources humaines nécessaires pour recruter, former et assurer le développement professionnel du personnel de cybersécurité.

B. Politiques, procédures et autres documents pertinents utilisés pour gérer les processus de cybersécurité, y compris :
   - Des politiques revues et mises à jour au moins une fois par an. Les risques émergents liés à la cyber peuvent nécessiter des révisions et des mises à jour plus fréquentes.
   - Un processus permettant de déterminer si les politiques et les procédures sont suffisantes pour soutenir les opérations de cybersécurité.
   - Des cadres largement adoptés (NIST, COBIT et autres) pour renforcer les processus de cybersécurité et les contrôles internes.

C. Rôles et responsabilités qui favorisent la réalisation des objectifs de cybersécurité, y compris une structure qui garantit que la fonction de cybersécurité relève d'un niveau de l'organisation qui a une visibilité suffisante pour obtenir le soutien de l'organisation.
   - Un processus d'évaluation périodique des connaissances, des compétences et des aptitudes du personnel chargé de la cybersécurité.

D. Preuve d'interactions avec les parties prenantes concernées (par exemple, la direction générale, les opérations, la gestion des risques, les ressources humaines,

le service juridique, la conformité, les fournisseurs stratégiques et autres), y compris la communication sur les cyber-risques existants et émergents et les vulnérabilités potentielles connues. Les preuves de communication peuvent être des comptes rendus de réunions, des rapports ou des courriels.

### *Considérations relatives à la gestion des risques*

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

A. La manière dont l'organisation évalue et gère les risques liés à la cybersécurité, y compris la manière dont les menaces et les vulnérabilités sont évaluées :
   - Initialement identifiées et signalées.
   - Analysées pour évaluer le risque d'atteinte des objectifs de l'organisation.
   - Atténuées, y compris les plans d'action visant à ramener le risque à un niveau acceptable.

Suivies, y compris un plan de communication continue jusqu'à ce que les menaces soient entièrement résolues.

B. La manière dont l'organisation obtient périodiquement des informations sur la gestion des risques de cybersécurité de la part des services fonctionnels, tels que les technologies de l'information, la gestion des risques d'entreprise, les ressources humaines, le service juridique, la conformité, les opérations, la comptabilité et les finances. Une équipe pluridisciplinaire de cybersécurité ou un comité de pilotage informatique peuvent être utilisés pour obtenir des informations.

C. La manière dont l'organisation a confié à une personne ou à une équipe l'obligation de rendre compte et la responsabilité de la gestion des risques liés à la cybersécurité.
   - Le(s) responsable(s) doit(vent) communiquer périodiquement (trimestriellement, mensuellement ou selon les besoins) à l'ensemble de l'organisation des mises à jour sur les risques de cybersécurité et peut(vent) également inclure les besoins en ressources pour les stratégies d'atténuation des risques.

D. Les processus de remontée des risques de cybersécurité, y compris la manière dont le niveau de menace ou de risque est évalué, attribué et classé par ordre de priorité. L'examen peut comprendre l'identification des éléments suivants :
   - Les niveaux de risque définis par l'organisation - tels que “élevé”, “modéré” ou “faible” - avec des explications détaillées de chaque niveau de risque et des procédures d'escalade pour chaque catégorie de risque.
   - Liste des risques de cybersécurité actuellement identifiés et état d'avancement de l'atténuation de chaque risque.
   - les exigences légales, réglementaires et de conformité applicables.

- Impacts des risques financiers et non financiers (par exemple, réputation).

E. Le processus de communication des risques de cybersécurité à la direction et aux employés, qui comprend :

   - Formation périodique (au moins une fois par an) des employés à la cybersécurité, par exemple en organisant des campagnes d'hameçonnage inopinées et simulées afin de tester et de suivre la sensibilisation de l'organisation.
   - Des mises à jour sur la résolution des problèmes de cybersécurité existants, avec les dates d'achèvement prévues.
   - le suivi des non-conformités, qui comprend des mises à jour à l'intention du Conseil et de la direction générale.
   - Réévaluer les menaces lorsque l'appétit pour le risque et la tolérance au risque de l'organisation changent.

F. Les processus mis en œuvre par l'organisation en matière de réponse aux incidents et de récupération, notamment :

   - Un plan documenté qui est revu et mis à jour au fur et à mesure de l'évolution des activités de l'organisation. Le plan doit comprendre :
     - La manière dont les incidents sont détectés et signalés.
     - La manière dont les incidents sont maîtrisés afin d'éviter d'autres dommages.
     - Comment l'organisation se rétablira et réagira pour reprendre ses activités.
     - Comment l'incident sera analysé afin d'en tirer des enseignements et d'éviter que de tels événements ne se reproduisent à l'avenir.

Tests périodiques (au moins une fois par an) (exercice de simulation) et communication des résultats aux dirigeants et aux parties prenantes concernées. Des plans d'action peuvent résulter de ces tests.

### *Considérations sur le processus de contrôle*

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

A. L'approche adoptée par la direction pour mettre en place un environnement de contrôle interne efficace en matière de cybersécurité, y compris :
   - Évaluer et mettre en œuvre les contrôles internes nécessaires pour atténuer les risques élevés et protéger les données sensibles, critiques, personnelles ou confidentielles, en s'appuyant sur le processus d'évaluation des risques de l'organisation.

- Déterminer les ressources nécessaires pour maintenir opérationnels les contrôles clés en matière de cybersécurité.
- Considérer les contrôles effectués par les fournisseurs comme faisant partie de l'environnement de contrôle, ce qui inclut l'examen des rapports des fournisseurs concernant leurs services de contrôle des organisations (SOC) avant le début de la relation commerciale et pendant toute la durée de celle-ci.
- Réaliser des tests périodiques visant à vérifier que les contrôles de cybersécurité fonctionnent de manière à atténuer les risques et à favoriser la réalisation des objectifs en matière de cybersécurité.

Examiner les processus permettant de remédier aux déficiences du contrôle interne ou de traiter les conclusions des évaluations réalisées par la fonction d'audit interne ou d'autres prestataires d'assurance (par exemple, les tests de pénétration).

B. Le processus de gestion des compétences de l'organisation pour le recrutement et la formation des professionnels de la cybersécurité, y compris la manière dont l'organisation identifie les possibilités de développer les capacités des professionnels de la cybersécurité à soutenir les connaissances techniques et à améliorer la sensibilisation de l'organisation aux questions émergentes.

Il s'agit par exemple de la participation à des formations, de l'implication dans des groupes de partage des connaissances et de la formation professionnelle continue qui comprend l'obtention de certifications dans le domaine de la cybersécurité.

C. Le processus mis en place par la direction pour identifier, hiérarchiser, surveiller et signaler les menaces et les vulnérabilités émergentes en matière de cybersécurité sur une base continue et axée sur les opérations quotidiennes. L'examen peut porter sur la mise en place de processus d'évaluation des menaces et des vulnérabilités liées aux technologies nouvelles ou émergentes, telles que l'utilisation de l'intelligence artificielle.

D. Processus et contrôles mis en place par la direction pour gérer et protéger les actifs informatiques tout au long de leur cycle de vie, y compris la sélection, l'utilisation, la maintenance et de décommissionnement des matériels, des logiciels et des services des fournisseurs. Le matériel comprend les serveurs, les équipements de réseau (tels que les routeurs ou les pare-feu), les ordinateurs de bureau, les ordinateurs portables, les téléphones cellulaires, les tablettes et les périphériques. Les logiciels comprennent les systèmes d'exploitation (tels que Windows), les logiciels de planification des ressources de l'entreprise (ERP), les applications, les programmes antivirus et autres. Les considérations matérielles et logicielles peuvent inclure :
   - L'utilisation par l'organisation du chiffrement, de logiciels antivirus, de la gestion des appareils mobiles, de mots de passe complexes, de réseaux privés virtuels (VPN) et de réseaux de confiance zéro (ZTN) pour l'authentification, et la mise à jour périodique des microprogrammes (firmware).
   - Processus de gestion des actifs qui garantit que les équipements informatiques fournis par l'entreprise possèdent une configuration de sécurité appropriée au

moment de sa mise à disposition et qu'ils sont correctement décommissionnés lorsque ces actifs sont retirés du service.

- Les contrôles liés aux bases de données qui comprennent la limitation de l'accès des utilisateurs et des administrateurs, l'utilisation du chiffrement, la sauvegarde et le test des bases de données, et la présence de contrôles de sécurité solides sur le réseau.
- Comment les menaces ou les vulnérabilités en matière de cybersécurité sont prises en compte dans le cycle de développement du système (SDLC).
- L'approche utilisée par le développement, la sécurité et les opérations (DevSecOps) pour s'assurer que le processus de développement de logiciels inclut la cybersécurité afin d'identifier les vulnérabilités de manière proactive.

E. Les processus utilisés pour renforcer la cybersécurité, y compris :
   - Configuration des paramètres de sécurité pour minimiser les risques de cybersécurité.
   - L'administration des appareils mobiles (y compris l'utilisation des messageries électroniques et des applications) est configurée pour atténuer les risques de cybersécurité et être gérée à distance si l'appareil d'un utilisateur est compromis.
   - L'utilisation du chiffrement pour les données "au repos", telles que les informations stockées sur un disque dur, ou les données "en transit", telles que le chiffrement des courriels.
   - Mise à jour des serveurs ou des logiciels (tels que les systèmes d'exploitation) avec les dernières versions de sécurité.
   - La gestion de l'accès des utilisateurs, comme l'utilisation de l'authentification multi-facteurs (MFA) et d'identifiants uniques avec des mots de passe complexes qui expirent périodiquement.
   - Contrôles de surveillance mis en place pour déterminer si la disponibilité et l'utilisation des ressources sont adéquates, ce qui permet d'examiner et d'analyser les problèmes potentiels de cybersécurité qui menacent les performances.

Intégration de la cybersécurité dans le cycle de développement (SDLC) afin d'identifier et de traiter les vulnérabilités en matière de cybersécurité avant que le logiciel ne soit mis en production.

F. Les contrôles liés au réseau qui sécurisent le périmètre de l'organisation, y compris la façon dont l'organisation utilise :
   - La segmentation du réseau.
   - Les pare-feu.
   - Les contrôles d'accès des utilisateurs.
   - Les limitations des connexions externes et internes.
   - Les contrôles relatifs à l'internet des objets (IoT) pour les réseaux interconnectés.

Les systèmes de détection/prévention des intrusions pour prévenir et détecter les attaques de cybersécurité et assurer la reprise.

G. Contrôles portant sur la sécurité des terminaux de communications (endpoints) , applicables à des services tels que le courrier électronique, les navigateurs internet, la vidéoconférence, les environnements de travail collaboratifs (Zoom, MS Teams et autres), les médias sociaux, les clouds et les protocoles de partage de fichiers. Les contrôles peuvent inclure la restriction de l'utilisation de certaines extensions de fichiers (comme les fichiers .exe) et l'authentification multi-facteurs pour le partage de fichiers.

# Annexe A. Exemples d'applications pratiques

Les exemples suivants décrivent des scénarios dans lesquels l'Exigence Thématique relative à la cybersécurité serait applicable :

**Exemple 1 : La cybersécurité est identifiée pour une mission incluse dans le plan d'audit interne.**

Lorsque la fonction d'audit interne finalise son processus de planification fondé sur les risques et inclut une ou plusieurs missions sur la cybersécurité dans le plan d'audit interne, l'Exigence Thématique est obligatoire lors de la réalisation de ces missions. La conformité peut être obtenue en incluant les exigences dans une ou plusieurs missions du plan d'audit interne.

La cybersécurité est un sujet vaste, et toutes les exigences de l'Exigence Thématique ne s'appliquent pas nécessairement à toutes les missions. Lorsque les auditeurs internes exercent leur jugement professionnel et déterminent qu'une ou plusieurs exigences de l'Exigence Thématique relative à la cybersécurité ne sont pas applicables et devraient donc être exclues d'une mission, ils doivent documenter et conserver les justifications de l'exclusion de ces exigences. Par exemple, l'exclusion de certaines exigences peut être justifiée par le fait que la fonction d'audit interne effectue diverses missions de cybersécurité par rotation ou qu'elle a déterminé que l'importance du risque dans la mission est faible.

**Exemple 2 : Des risques liés à la cybersécurité sont identifiés au cours d'une mission d'audit qui n'est pas centrée sur la cybersécurité**.

Les auditeurs internes peuvent identifier des risques de cybersécurité lors de l'évaluation d'un processus qui n'est pas directement lié à la cybersécurité. Par exemple, les auditeurs internes peuvent évaluer le processus de comptabilité fournisseurs dans le cadre d'une mission qui n'est pas centrée sur la cybersécurité et ne pas identifier les risques de cybersécurité comme faisant partie du champ d'application lors de la planification de la mission. Cependant, après avoir effectué la revue initiale, les auditeurs internes déterminent que ces risques devraient être inclus dans le périmètre de la mission ; par exemple, ils identifient des risques de cybersécurité liés à la soumission en ligne d'une demande initiale de bon de commande (Norme 13.2 Évaluation des risques dans le cadre de la mission).

Une fois que les risques pertinents ont été identifiés, les auditeurs internes doivent examiner l'Exigence Thématique relative à la cybersécurité et déterminer quelles sont les exigences applicables. Dans cet exemple, ils pourraient exclure le processus de gouvernance de la cybersécurité ou le processus de gestion des risques liés à la cybersécurité. Ils doivent

documenter dans les dossiers de la mission les justifications pour lesquelles les autres exigences de l'Exigence Thématique relative à la cybersécurité ont été exclues et conserver la documentation.

**Exemple 3 : Une mission de cybersécurité qui n'était pas initialement prévue dans le plan d'audit interne est demandée**.

Des parties prenantes telles que le Conseil, la direction ou une autorité de régulation peuvent demander aux auditeurs internes de réaliser des évaluations de la cybersécurité en dehors du plan d'audit initial. Par exemple, lorsque des organisations sont la cible d'une cyberattaque, le Conseil peut demander à l'audit interne d'effectuer une mission d'évaluation des contrôles de cybersécurité. L'Exigence Thématique est applicable, les exigences doivent être évaluées et toute exclusion doit être documentée.

# Annexe B. Correspondance avec les Référentiels

L'organisation peut avoir son propre cadre en matière de cybersécurité, en utilisant les référentiels de gestion des risques et de gouvernance telles que COBIT ou NIST. Les auditeurs internes peuvent avoir déjà élaboré des programmes d'audit et des procédures de test fondés sur ces cadres. Les auditeurs internes doivent rapprocher les tests de contrôle de la cybersécurité qu'ils prévoient d'effectuer de l'Exigence Thématique afin de s'assurer que la couverture est adéquate. Le tableau ci-dessous établit une correspondance entre l'Exigence Thématique relative à la cybersécurité et trois cadres de référence couramment utilisés : NIST Cybersecurity Framework 2.0, COBIT 2019 et NIST 800-53. Ces cadres ont été mis en correspondance car ils sont disponibles gratuitement.

| Exigences en matière de gouvernance | Cadre de référence | | |
|---|---|---|---|
| | NIST CSF 2.0 | NIST 800-53 | COBIT 2019 |
| **A.** Une stratégie et des objectifs formels en matière de cybersécurité sont établis et périodiquement mis à jour. Des mises à jour sur la réalisation des objectifs de cybersécurité sont périodiquement communiquées et examinées par le Conseil , y compris les ressources et les considérations budgétaires à l'appui de la stratégie de cybersécurité. | GV.RM-01 ; GV.RM-02 ; GV.RM-03 ; GV.RM-04 ; GV.OC-02 ; GV.RR-03 ; GV.RR-04 ; GV.PO-01 ; GV.PO-02 ; GV.OV-01 ; GV.OV-03 | PM-1, PM-4 ; AT-2 ; AT-3 ; PM-9 ; PM-28 | EDM01 ; EDM03 ; EDM04 ; APO06 ; APO01 ; APO10 ; APO12 |
| **B.** Des politiques et des procédures relatives à la cybersécurité sont établies, périodiquement mises à jour et renforcent l'environnement de contrôle. | GV.PO-01 ; GV.PO-02 ; GV.OV-01 ; GV.OV-02 ; GV.OV-03 ; GV.SC-01 ; GV.SC-03 ; GV.RR-03 | AC-1, PM-9 ; AC-1 ; AT-1 ; CA-1 ; CM-1 ; IA-1 ; IR-1 ; MP-1 ; PE-1 | EDM01 ; EDM02 ; EDM03 ; APO01 ; APO11 |

| | | | |
|---|---|---|---|
| **C.** Les rôles et les responsabilités à l'appui des objectifs de cybersécurité sont définis et il existe un processus permettant d'évaluer périodiquement les connaissances, les compétences et les aptitudes des personnes qui remplissent ces rôles. | GV.RR-02 ; GV.RR-04 ; GV.SC-02 ; GV.OC-02 | PM-13 ; AT-2 ; AT-3 | EDM02 ; APO01 ; APO07 |
| **D.** Les parties prenantes concernées sont invitées à examiner les vulnérabilités existantes et les menaces émergentes dans le domaine de la cybersécurité et à prendre des mesures en conséquence. Les parties prenantes comprennent la direction générale, les opérations, la gestion des risques, les ressources humaines, le service juridique, la conformité, les fournisseurs et d'autres acteurs. | GV.OC-02 ; GV.RM-01 ; GV.RM-05 ; GV.RM-07 ; GV.OV-03 ; GV.SC-03 | AC-1 ; CM-1 | EDM05 ; EDM01.01 ; EDM03 ; MEA01.02 ; APO01 ; APO08 ; APO11 ; APO13 ; MEA02 |
| **Exigences en matière de gestion des risques** | **NIST CSF 2.0** | **NIST 800-53** | **COBIT 2019** |
| **A.** Les processus d'évaluation et de gestion des risques de l'organisation comprennent l'identification, l'analyse, l'atténuation et le suivi des menaces liées à la cybersécurité et de leurs effets sur la réalisation des objectifs stratégiques. | GV.RM-01 ; GV.RM-03 ; GV.OC-01 | AT-1 ; PM-9 ; PM-28 | EDM03 ; APO01 ; APO10 ; APO12 |
| **B.** La gestion des risques liés à la cybersécurité est effectuée dans l'ensemble de l'organisation, ce qui peut inclure les domaines suivants : technologies de l'information, gestion des risques d'entreprise, ressources humaines, services juridiques, conformité, opérations, chaîne d'approvisionnement, comptabilité, finances, etc. | GV.RM-01 ; GV.RM-05 ; GV.RR-01 ; GV.RR-02 ; GV.OC-03 ; GV.SC-07 | PM-29 ; AT-1 ; PM-9 ; PM-28 | EDM03 ; APO01 ; APO10 ; APO12 |

| | | | |
|---|---|---|---|
| **C.** 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 est désignée pour contrôler et rendre compte périodiquement de la manière dont les risques liés à la cybersécurité sont gérés, y compris les ressources nécessaires pour atténuer les risques et identifier les nouvelles menaces en matière de cybersécurité. | GV.RR-01 ; GV.RR-02 ; GV.RR-03 ; GV.0V-01 ; GV.OV-02 ; GV.OV-03 | PM-9 ; PM-29 | EDM03 ; APO01 ; APO10 ; APO12 |
| **D.** 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 réglementaires applicables. Les incidences financières et non financières du risque de cybersécurité doivent être prises en considération. | GV.RM ; ID.RA ; RS.MA-04 | CA-7 ; RA-3 ; RA-7 | EDM03 ; APO01, APO10 ; APO12 |
| **E.** Un processus est mis en place pour sensibiliser la direction et les employés aux risques liés à la cybersécurité et pour que la direction examine périodiquement les problèmes, les lacunes, les déficiences ou les défaillances des contrôles, en établissant des rapports et en prenant des mesures correctives. | PR.AT ; GV.RR.01 ; GV.RR-04 ; GV.PO | AT-2 | APO01 ; APO02 ; EDM03 ; MEA03 |

| | | | |
|---|---|---|---|
| **F.** L'organisation a mis en place un processus de réponse et de rétablissement en cas d'incident de cybersécurité qui comprend la détection, l'endiguement, le rétablissement et l'analyse post-incident. Le processus de réponse et de récupération en cas d'incident est testé périodiquement. | RS ; RC | IR-4 ; IR-5 ; IR-6 ; IR-7 ; IR-8 ; IR-10 ; SA-15 | DSS02 ; DSS03 ; DSS04 ; DSS05.07 |
| **Exigences du processus de contrôle** | **NIST CSF 2.0** | **NIST 800-53** | **COBIT 2019** |
| **A.** Un processus est mis en place pour garantir que des contrôles internes et des contrôles effectués par des fournisseurs sont en place pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes et des données de l'organisation. Les contrôles sont évalués périodiquement afin de déterminer s'ils fonctionnent d'une manière qui favorise la réalisation des objectifs de l'organisation en matière de cybersécurité et la résolution rapide des problèmes. | ID.IM-01 ; ID.IM-02 ; ID.IM-03 ; PR ; DE ; RS ; RC ; ID.RA06 ; GV.RM-05 ; GV.SC ; ID.IM-02 ; RS.MA-01 ; DE.CM-06 | AC-3 ; AC-4 ; AC-10 ; AC-13 ; AC-17 ; PM-30 ; RA-3 ; SA-9 ; SR-2 | MEA02 ; MEA04 ; EDM03 ; APO09 ; APO10 ; DSS01 |
| **B.** Un processus de gestion des talents est mis en place et revu périodiquement pour les opérations de cybersécurité ; il prévoit des possibilités de formation pour développer et maintenir les compétences techniques. | PR.AT-01 ; PR.AT-02 ; GV.RR-03 | AT-2 ; AT-3 ; IR-2 ; PM-14 | APOO7 ; DSS04 |
| **C.** Un processus est mis en place pour surveiller et signaler en permanence les nouvelles menaces et vulnérabilités en matière de cybersécurité et pour recenser, hiérarchiser et mettre en œuvre les possibilités d'amélioration des opérations de cybersécurité. | ID.RA-02 ; ID.RA-03, ID.RA-04 | CA-7 ; PM-31 ; RA-5 | DSS03.05 |

| | | | |
|---|---|---|---|
| **D.** La cybersécurité est incluse dans la gestion du cycle de vie (sélection, utilisation, maintenance et mise hors service) de tous les actifs informatiques, y compris le matériel, les logiciels et les services des fournisseurs. | ID.AM ; PR.PS-03 ; PR.IR ; DE.CM-09 ; ID.AM-08 ; ID.RA-09 ; PR.PS-06 | AU-9 ; CM-7 ; SC-49 ; SC-51 ; CM-2 ; SA-3 ; SA-10 ; SA-15 ; SA-17 ; SA-20 ; AU-6 ; IR-7 | DSS05.03 ; BAI03 ; BAI09 ; BAI03 ; BAI11 ; DSS05.01 ; DSS02 ; DSS03 ; DSS06.06 |
| **E.** Des processus sont mis en place pour promouvoir la cybersécurité, notamment en ce qui concerne la configuration, l'administration des dispositifs destinés aux utilisateurs finals, le cryptage, l'application de correctifs, la gestion de l'accès des utilisateurs et le contrôle de la disponibilité et des performances. Les considérations de cybersécurité sont prises en compte dans le développement des logiciels (DevSecOps). | PR.PS-01 ; PR.PS-06 ; PR.DS-01 ; PR.DS-02 ; PR.PS-05 ; DE.CM-03 | CM-6 ; SI-2 ; AC-3 ; CA-7 ; SA-4 ; AC-16 ; AC-18 | BAI10 ; DSS05 ; DSS06.03 ; DSS01.03 ; MEA01 |
| **F.** Des contrôles liés au réseau sont mis en place, tels que les contrôles d'accès au réseau et la segmentation, l'utilisation et l'emplacement des pare-feu, les connexions limitées depuis et vers les réseaux externes, le réseau privé virtuel (VPN)/l'accès au réseau de confiance zéro (ZTNA), l'inclusion des contrôles du réseau de l'internet des objets (IoT) et les systèmes de détection/prévention des intrusions (IDS et IPS). | PR.IR ; DE.CM-01 | AC-6 ; AC-17 ; AC-18 ; AC-20 ; SC-7 ; SC-10 ; CA-8 | DSS05.02 |
| **G.** Des contrôles de sécurité des communications au niveau des terminaux (endpoints) sont établis pour les services tels que le courrier électronique, les navigateurs internet, la vidéoconférence, les environnements de travail collaboratifs, les médias sociaux, le cloud et les protocoles de partage de fichiers. | PR.DS-01 ; PR.DS-02 ; PR.DS-10 ; PR.IR | AC-2 ; AC-16 ; AU-10 ; CA-3 ; SI-8 ; SI-20 ; SC-8 | BAI10 |

# Annexe C. Outil de documentation optionnel

Les auditeurs internes sont censés exercer leur jugement professionnel pour déterminer l'applicabilité des exigences sur la base de l'évaluation des risques et documenter de manière appropriée l'exclusion de certaines exigences. L'Exigence Thématique peut être documentée dans le plan d'audit interne ou dans les documents de travail de la mission en fonction du jugement professionnel de l'auditeur. Une ou plusieurs missions d'audit interne peuvent couvrir les exigences. En outre, toutes les exigences peuvent ne pas être applicables. Le formulaire imprimable ci-dessous permet de documenter la conformité à l'exigence thématique relative à la cybersécurité, mais son utilisation n'est pas obligatoire.

### *Cybersécurité - Gouvernance*

| Exigence | Couverture exécutée ou justification de l'exclusion | Référence de la documentation |
|---|---|---|
| **A.** Une stratégie et des objectifs formels en matière de cybersécurité sont établis et périodiquement mis à jour. Des mises à jour sur la réalisation des objectifs de cybersécurité sont périodiquement communiquées et examinées par le conseil d'administration, y compris en ce qui concerne les ressources et les considérations budgétaires à l'appui de la stratégie de cybersécurité. | | |
| **B.** Des politiques et des procédures relatives à la cybersécurité sont établies, périodiquement mises à jour et renforcent l'environnement de contrôle. | | |
| **C.** Les rôles et les responsabilités à l'appui des objectifs de cybersécurité sont définis et il existe un processus permettant d'évaluer périodiquement les connaissances, les compétences et les aptitudes des personnes qui assument ces rôles. | | |

| Exigence | Couverture exécutée ou justification de l'exclusion | Référence de la documentation |
|---|---|---|
| **D.** Les parties prenantes concernées sont invitées à examiner les vulnérabilités existantes et les menaces émergentes dans le domaine de la cybersécurité et à prendre des mesures en conséquence. Les parties prenantes comprennent la direction générale, les opérations, la gestion des risques, les ressources humaines, le service juridique, la conformité, les fournisseurs et d'autres acteurs. | | |

## *Cybersécurité - Gestion des risques*

| Exigence | Couverture exécutée ou justification de l'exclusion | Référence de la documentation |
|---|---|---|
| **A.** Les processus d'évaluation et de gestion des risques de l'organisation comprennent l'identification, l'analyse, l'atténuation et le suivi des menaces liées à la cybersécurité et de leurs effets sur la réalisation des objectifs stratégiques. | | |
| **B.** La gestion des risques liés à la cybersécurité est menée dans l'ensemble de l'organisation et peut inclure les domaines suivants : technologies de l'information, gestion des risques d'entreprise, ressources humaines, affaires juridiques, conformité, opérations, chaîne d'approvisionnement, comptabilité, finances, etc. | | |

| Exigence | Couverture exécutée ou justification de l'exclusion | Référence de la documentation |
|---|---|---|
| **C.** L'obligation de rendre compte et la responsabilité de la gestion des risques liés à la cybersécurité sont établies. Une personne ou une équipe est désignée pour contrôler et rendre compte périodiquement de la manière dont les risques liés à la cybersécurité sont gérés, y compris les ressources nécessaires pour atténuer les risques et identifier les nouvelles menaces en matière de cybersécurité. | | |
| **D.** Un processus est mis en place pour faire remonter rapidement tout risque de cybersécurité (émergent ou déjà identifié) qui atteint un niveau inacceptable selon les lignes directrices établies par l'organisation en matière de gestion des risques ou les exigences légales et réglementaires applicables. Les incidences financières et non financières du risque de cybersécurité devraient être prises en compte. | | |
| **E.** Un processus est mis en place pour sensibiliser la direction et les employés aux risques liés à la cybersécurité et pour que la direction examine périodiquement les problèmes, les lacunes, les déficiences ou les défaillances des contrôles, en établissant des rapports et en prenant des mesures correctives en temps utile. | | |

| Exigence | Couverture exécutée ou justification de l'exclusion | Référence de la documentation |
|---|---|---|
| **F.** L'organisation a mis en place un processus de réponse et de rétablissement en cas d'incident de cybersécurité, comprenant la détection, l'endiguement, le rétablissement et l'analyse post-incident. Le processus de réponse et de récupération en cas d'incident est testé périodiquement. | | |

## *Cybersécurité - Processus de contrôle*

| Exigence | Couverture exécutée ou justification de l'exclusion | Référence de la documentation |
|---|---|---|
| **A.** Un processus est mis en place pour garantir que des contrôles internes et des contrôles effectués par des fournisseurs sont en place pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes et des données de l'organisation. Des évaluations sont effectuées périodiquement pour déterminer si les contrôles fonctionnent d'une manière qui favorise la réalisation des objectifs de l'organisation en matière de cybersécurité et la résolution rapide des problèmes. | | |
| **B.** Un processus de gestion des talents est mis en place, qui comprend des formations visant à développer et à maintenir les compétences techniques liées aux opérations de cybersécurité. Ce processus fait l'objet d'un examen périodique. | | |

| Exigence | Couverture exécutée ou justification de l'exclusion | Référence de la documentation |
|---|---|---|
| **C.** Un processus est mis en place pour surveiller et signaler en permanence les nouvelles menaces et vulnérabilités en matière de cybersécurité et pour recenser, hiérarchiser et mettre en œuvre les possibilités d'amélioration des opérations de cybersécurité. | | |
| **D.** La cybersécurité est incluse dans la gestion du cycle de vie (sélection, utilisation, maintenance et mise hors service) de tous les actifs informatiques, y compris le matériel, les logiciels et les services des fournisseurs. | | |
| **E.** Des processus sont mis en place pour promouvoir la cybersécurité, notamment en ce qui concerne la configuration, l'administration des dispositifs destinés aux utilisateurs finals, le chiffrement, l'application de correctifs, la gestion de l'accès des utilisateurs et le contrôle de la disponibilité et des performances. Les considérations de cybersécurité sont prises en compte dans le développement des logiciels (DevSecOps). | | |
| **F.** Des contrôles liés au réseau sont mis en place, tels que les contrôles d'accès au réseau et la segmentation ; l'utilisation et l'emplacement des pare-feu ; les connexions limitées depuis et vers les réseaux externes ; le réseau privé virtuel (VPN)/l'accès au réseau de confiance zéro (ZTNA), les contrôles du réseau de l'internet des objets (IoT), et les systèmes de détection/prévention des intrusions (IDS et IPS). | | |

| Exigence | Couverture exécutée ou justification de l'exclusion | Référence de la documentation |
|---|---|---|
| **G.** Des contrôles de sécurité des communications au niveau des terminaux sont établis pour des services tels que le courrier électronique, les navigateurs internet, la vidéoconférence, les environnements de travail collaboratifs, les médias sociaux, le cloud et les protocoles de partage de fichiers. | | |

## À propos de l'Institut des auditeurs internes

L'Institut des auditeurs internes (IIA) est une association professionnelle internationale qui compte plus de 255 000 membres dans le monde et a délivré plus de 200 000 certifications Certified Internal Auditor® (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 : www.theiia.org.

## Clause de non-responsabilité



## Droit d'auteur



Février 2025

The Institute of
Internal Auditors

**Global Headquarters**
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101