Cybersécurité

Topical Requirement

Exigence Thématique

The Institute of
Internal Auditors

Exigence Thématique en matière de cybersécurité

Le Cadre international des pratiques professionnelles (International Professional Practices Framework®) comprend les Normes internationales de l'audit interne (Global Internal Audit Standards™), les Exigences Thématiques et les Lignes directrices internationales. Les Exigences Thématiques sont obligatoires et doivent être utilisées conjointement avec les Normes, qui constituent la base faisant autorité pour les pratiques requises.

Les Exigences Thématiques définissent des attentes claires pour les auditeurs internes en fixant un niveau de référence minimum pour l'audit de thèmes de risques spécifiques. Le profil de risque de l'organisation peut rendre nécessaire pour les auditeurs internes de prendre en compte d'autres aspects du sujet.

La conformité aux Exigences Thématiques renforcera la cohérence des services d'audit interne et améliorera la qualité et la fiabilité des services et des résultats de l'audit interne. En fin de compte, les Exigences Thématiques réhaussent la profession d'audit interne.

Les auditeurs internes doivent appliquer les Exigences Thématiques conformément aux Normes internationales de l'audit interne. La conformité aux Exigences Thématiques est obligatoire pour les services d'assurance et recommandée pour les services de conseil.

L'Exigence Thématique est applicable lorsque le sujet est l'un des suivants :

A. L'objet d'une mission dans le plan d'audit interne.
B. Identifié lors de l'exécution d'une mission.
C. L'objet d'une demande de mission ne figurant pas dans le plan d'audit interne initial.

L'applicabilité de chaque exigence de l'Exigence Thématique doit être évaluée. Les éléments probants de ces évaluations doivent être documentés et conservés. Toutes les exigences ne s'appliquent pas nécessairement à chaque mission ; si des exigences sont exclues, une justification doit être consignée dans la documentation et conservée. La conformité à l'Exigence Thématique est obligatoire et sera évaluée lors des évaluations de la qualité.

Pour plus d'informations, voir le guide de l'utilisateur de l'Exigence Thématique de cybersécurité.

Cybersécurité

Le National Institute of Standards and Technology (NIST) définit la cybersécurité simplement comme "la capacité de protéger ou de défendre l'utilisation du cyberespace contre les cyberattaques". La cybersécurité est un sous-ensemble de la sécurité 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".

La cybersécurité réduit les risques en renforçant l'environnement de contrôle d'ensemble et en protégeant les actifs informationnels d'une organisation contre les accès non autorisés, les perturbations, les altérations ou les destructions. 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.

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

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. Les exigences constituent une base minimale pour l'évaluation de la cybersécurité au sein d'une organisation.

GOUVERNANCE : Évaluer la gouvernance de la cybersécurité

Exigences :

Les auditeurs internes doivent évaluer les éléments suivants en relation avec la gouvernance de la cybersécurité de l'organisation :

D. 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.

E. Des politiques et des procédures relatives à la cybersécurité sont établies et périodiquement mises à jour afin de renforcer l'environnement de contrôle.

F. Les rôles et les responsabilités qui soutiennent les objectifs de cybersécurité sont établis et un processus existe pour évaluer périodiquement les connaissances, les compétences et les aptitudes des personnes occupant ces rôles.

Les parties prenantes concernées sont invitées à discuter et à agir sur les vulnérabilités existantes et les menaces émergentes dans l'environnement de la cybersécurité. Il s'agit notamment de la direction générale, des opérations, de la gestion des risques, des ressources humaines, du service juridique, de la conformité, des fournisseurs, etc.

GESTION DES RISQUES : Évaluation de la gestion des risques liés à la cybersécurité

Exigences :

Les auditeurs internes doivent évaluer les éléments suivants en relation avec la gestion du risque de cybersécurité de l'organisation :

G. 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 impacts sur la réalisation des objectifs stratégiques.

H. 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 de l'entreprise, ressources humaines, juridique, conformité, opérations, chaîne d'approvisionnement, comptabilité, finances, etc.

I. Les rôles et responsabilités en matière de gestion des risques liés à la cybersécurité sont établis. Une personne ou une équipe est désignée pour suivre 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.

J. 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 doivent être prises en compte.

K. 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 de contrôle, en les signalant et en y remédiant dans des délais adaptés..

L'organisation a mis en place un processus de réponse aux incidents de cybersécurité et de reprise qui comprend la détection, l'endiguement, la reprise et l'analyse post-incident. Le processus de réponse et de reprise en cas d'incident est testé périodiquement.

CONTRÔLES : Évaluation des processus de contrôle de la cybersécurité

Exigences :

Les auditeurs internes doivent évaluer les éléments suivants en relation avec les processus de contrôle de la cybersécurité de l'organisation :

L. Un processus est mis en place pour s'assurer que les contrôles internes et les contrôles effectués par les fournisseurs sont en place pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes et des données de l'organisation. Des évaluations sont conduites périodiquement pour déterminer si les contrôles fonctionnent de manière à favoriser la réalisation des objectifs de l'organisation en matière de cybersécurité et la résolution rapide des problèmes.

M. 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.

N. Un processus est mis en place pour surveiller et signaler en continu les nouvelles menaces et vulnérabilités en matière de cybersécurité et pour identifier, hiérarchiser et mettre en œuvre les opportunités d'amélioration des opérations de cybersécurité.

O. 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.

P. Des processus sont mis en place pour renforcer la cybersécurité, notamment la configuration, l'administration des appareils des utilisateurs finaux, le chiffrement, le déploiement de correctifs, la gestion des accès des utilisateurs et le suivi de la disponibilité et des performances. Les considérations de cybersécurité sont prises en compte dans le développement des logiciels (DevSecOps).

Q. Des contrôles liés au réseau sont mis en place, tels que les contrôles et la segmentation de l'accès au réseau ; 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).

R. Des contrôles de sécurité des communications au niveau des terminaux (endpoints) sont établis pour des services tels que le courrier électronique, les navigateurs internet, la vidéoconférence, la messagerie, 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. Fondée en 1941, l'IIA est reconnue 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, consultez le site www.theiia.org.

Droit d'auteur

Février 2025

The Institute of Internal Auditors

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