Résilience Organisationnelle

Exigence Thématique

Topical Requirement

Traduit en collaboration par :

The Institute of Internal Auditors

IFACI IIA France

The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

Exigence Thématique – Résilience Organisationnelle

Le Cadre de Référence International des Pratiques Professionnelles (International Professional Practices Framework®) comprend les Normes internationales d'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 font autorité en matière de pratiques requises.

Les Exigences Thématiques définissent des attentes claires pour les auditeurs internes en établissant un niveau minimal pour l'audit des domaines comportant des risques spécifiques. Le profil de risque de l'organisation peut obliger les auditeurs internes à prendre en considération d'autres aspects du sujet, notamment les règlementations locales.

La conformité aux Exigences Thématiques renforcera la cohérence des activités d'audit interne et améliorera la qualité, la fiabilité et les résultats des services d'audit interne. En fin de compte, les Exigences Thématiques contribuent à rehausser le niveau professionnel de l'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 missions d'assurance et recommandée pour les missions de conseil.

L'Exigence Thématique est applicable lorsque le thème correspond à l'un des éléments suivants :

- Le thème d'une mission inscrite au plan d'audit interne.
- Le thème a été identifié lors de la réalisation d'une mission.
- Le thème d'une mission demandée qui ne figurait pas dans le plan d'audit interne initial.

Toutes les exigences individuelles ne s'appliquent pas nécessairement à chaque mission, et certaines peuvent être satisfaites par d'autres approches. Si une exigence est exclue ou remplacée par d'autres exigences réglementaires ou contractuelles, ou si elle est traitée par la mise en œuvre de procédures conformes aux Normes internationales d'audit interne, la justification doit être documentée et conservée. La conformité sera évaluée dans le cadre des évaluations de la qualité.

Pour plus d'informations, consulter le Guide de l'utilisateur de l'Exigence Thématique relatif à la Résilience organisationnelle.

Résilience Organisationnelle

La résilience organisationnelle est définie par l'Organisation Internationale de Normalisation (ISO) comme la « capacité d'une organisation à absorber et à s'adapter à un environnement changeant » (ISO 22316:2017). Bien que cette définition constitue une orientation claire, dans la pratique, les organisations varient considérablement dans leur manière d'anticiper, de réagir, de s'adapter et de se remettre des changements et des perturbations. Comme la résilience organisationnelle couvre des dimensions stratégiques, opérationnelles, technologiques, humaines, sociales et financières, certaines organisations sont en mesure d'absorber efficacement les changements, tandis que d'autres éprouvent des difficultés ou choisissent des approches différentes face à l'incertitude.

La résilience organisationnelle est un concept global qui traite des risques susceptibles de perturber ou de compromettre de manière significative la capacité d'une organisation à fournir ses produits et services essentiels, à maintenir la confiance des parties prenantes ou à atteindre ses objectifs stratégiques. Ces risques peuvent découler d'événements soudains (tels que des catastrophes naturelles, des cyberattaques et des conflits géopolitiques), de pressions environnementales prolongées (telles que la rareté des ressources et les crises de santé publique) ou de changements dans le contexte externe (tels que des perturbations technologiques, des changements réglementaires et une dégradation de la réputation).

Ces risques peuvent également correspondre à des changements graduels ou à des pressions qui s'accumulent lentement et qui, au fil du temps, compromettent la stabilité et la capacité d'adaptation de l'organisation. Ces risques progressifs sont souvent négligés. Les organisations résilientes anticipent et s'adaptent aux risques tant soudains que plus subtils afin d'assurer leur performance.

Les facteurs de risque inhérents qui accentuent les menaces pensant sur la résilience comprennent notamment des opérations très complexes, des chaînes d'approvisionnement mondialisées, des infrastructures ou des systèmes de données centralisés, une disponibilité limitée de la main-d'œuvre, des conditions de marché volatiles et une forte dépendance envers des tiers critiques ou des zones géographiques spécifiques. Les organisations évoluant dans des secteurs à haute fiabilité ou soumises à une surveillance réglementaire accrue peuvent également être exposées à des risques intrinsèquement plus élevés en raison de leur impact sur le public et de leurs obligations de conformité.

La résilience organisationnelle repose sur la gestion des risques avant, pendant et après une perturbation. Les auditeurs internes évaluent généralement les processus et contrôles en technologies de l'information (TI) liés à la continuité d'activité et à la reprise après sinistre. Un plan de continuité d'activité définit le détail des mesures qu'une organisation met en œuvre pour maintenir ses fonctions essentielles et revenir à un fonctionnement normal en cas de sinistre. Un plan de reprise après sinistre décrit la manière dont une organisation rétablit ses systèmes informatiques, ses données critiques ses opérations après un événement perturbateur afin de reprendre le cours normal de ses activités.

La résilience organisationnelle, qui englobe ces deux plans, nécessite une planification stratégique, une gestion des risques d'entreprise, un leadership et une culture efficaces, ainsi que des processus de contrôle à l'échelle de l'organisation. Des processus de contrôle robustes en matière de résilience organisationnelle permettent non seulement d'anticiper, de se préparer, de réagir et de s'adapter continuellement aux changements, mais aussi d'assurer la pérennité et la performance de l'organisation.

Évaluation de la gouvernance, de la gestion des risques et des processus de contrôle de la résilience organisationnelle

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 liés à la résilience organisationnelle. Les exigences constituent un seuil minimal pour l'évaluation de la résilience organisationnelle.

Gouvernance

Exigences

Les auditeurs internes doivent évaluer les aspects suivants de la gouvernance de la résilience organisationnelle :

A. Une stratégie organisationnelle formelle intégrant la résilience est établie par la direction, adoptée et supervisée par le Conseil, et comprend les éléments opérationnels, technologiques et financiers nécessaires pour gérer les changements et assurer la continuité des opérations. Les objectifs de résilience s'alignent sur l'approche d'ensemble de l'organisation en matière de gestion des risques.

B. Des mises à jour sur l'atteinte des objectifs de résilience sont communiquées périodiquement au Conseil pour examen. Cela garantit que la résilience est intégrée à la supervision stratégique, aux processus de planification à long terme, à la planification de la relève et à la culture de l'organisation, y compris dans les considérations de ressources et de budget nécessaires au soutien des activités essentielles.

C. Des politiques et procédures relatives aux processus critiques (opérationnels, technologiques et financiers) sont établies et font l'objet de revue, de tests et de mises à jour périodiques afin de renforcer l'environnement de contrôle.

D. Une structure de gestion de crise est en place pour superviser et soutenir les objectifs de résilience organisationnelle. Elle comprend les hiérarchies décisionnelles, les protocoles de communication et d'escalade, ainsi que les rôles et responsabilités des dirigeants et des équipes opérationnelles.

E. Un processus est en place pour valider périodiquement les compétences nécessaires à la réussite en matière de résilience et réévaluer les compétences des personnes occupant des rôles clés dans les processus de résilience.

F. Un processus est en place afin de s'assurer que toutes les parties prenantes internes et externes pertinentes sont identifiées, priorisées et mobilisées dans la mise en place de structures d'information et de reporting pour l'atteinte des objectifs de résilience organisationnelle. Les parties prenantes peuvent inclure la direction générale, les opérations, la gestion des risques, les technologies de l'information, la chaîne d'approvisionnement et les achats, les installations, les ressources humaines, la finance, le service juridique, les prestataires de services d'assurance (y compris l'audit interne), la conformité, les relations publiques, les fournisseurs critiques, les clients, les autorités de réglementation et d'autres.

Gestion des risques

Exigences

Les auditeurs internes doivent évaluer les aspects suivants de la gestion des risques liés à la résilience de l'organisation :

A. Les risques liés à la résilience organisationnelle sont périodiquement identifiés, évalués et gérés à l'échelle de l'organisation. Les risques liés à la résilience sont mis en correspondance avec les objectifs stratégiques de l'organisation. Le processus de gestion du risque liés à la résilience comprend l'évaluation des processus clés.

B. L'imputabilité et la responsabilité en matière de gestion des risques liés à la résilience organisationnelle sont clairement définies. Une personne ou une équipe désignée est chargée d'assurer le suivi régulier de la gestion des risques liés à la résilience organisationnelle et d'en rendre compte, y compris les ressources nécessaires à l'atténuation des risques et à l'identification des menaces émergentes.

C. Un processus est en place pour surveiller les niveaux de risque liés à la résilience organisationnelle (émergents ou déjà identifiés) et escalader rapidement ceux qui atteignent un niveau jugé inacceptable, conformément aux lignes directrices de gestion des risques et à la tolérance au risque de l'organisation, ou aux exigences légales et réglementaires applicables. Les impacts des risques liés à la résilience organisationnelle sont pris en compte.

D. La direction a mis en place et teste périodiquement un processus de réponse et de reprise en cas de crises, de perturbations et d'urgences. Le processus de réponse aux incidents et de reprise comprend la détection, la priorisation, l'endiguement, la reprise et l'analyse post-incident. L'approche de réponse aux incidents comprend des analyses de scénarios ainsi que des tests de résistance périodiques (stress testing) face à un éventail d'événements perturbateurs.

Processus de contrôle

Exigences

Les auditeurs internes doivent évaluer les aspects suivants des processus de contrôle liés à la résilience organisationnelle :

A. Un processus est en place pour identifier les tiers critiques (fournisseurs et prestataires) et déterminer les niveaux de stocks minimums requis pour maintenir les opérations essentielles. Le processus comprend également le maintien d'une liste à jour de fournisseurs alternatifs.

B. Les données critiques pour les opérations sont identifiées et classifiées. La classification des données comprend l'identification de l'endroit où elles se trouvent, des personnes qui doivent y avoir accès, de la manière dont elles sont accessibles, ainsi que leur sauvegarde et leur capacité à être récupérées en cas d'urgence.

C. Des contrôles informatiques essentiels ainsi qu'une surveillance continue sont mis en place afin d'atténuer les risques liés à la sécurité de l'information (y compris les risques cyber) et de protéger les données sensibles lors de crises, de perturbations ou

d'urgences. Les contrôles et la surveillance continue comprennent la veille sur les menaces en temps réel ainsi que la restriction de l'accès aux seuls utilisateurs autorisés.

D. Les actifs informatiques critiques sont inventoriés. Les actifs comprennent le matériel, les logiciels et les services nécessaires pour soutenir les opérations lors de crises, de perturbations et d'urgences.

E. Des plans de continuité des activités et de reprise après sinistre sont établis et définissent les rôles du personnel désigné et des équipes de reprise. Les plans sont testés périodiquement (par exemple au moyen d'un "exercice sur table") et les résultats, y compris les possibilités d'amélioration, sont communiqués au Conseil et à la direction générale.

F. Un processus est en place pour adapter l'environnement de travail en cas de crises, de perturbations ou d'urgences.

G. Un processus est en place pour surveiller et signaler en continu les menaces et vulnérabilités émergentes susceptibles d'affecter la résilience organisationnelle. Ce processus permet d'identifier, de prioriser et de mettre en œuvre des améliorations des activités de résilience organisationnelle, y compris mécanismes de signalement et de collecte de renseignements sur les risques.

H. Un processus est en place pour sensibiliser et former le personnel à la résilience organisationnelle, en veillant à ce qu'il connaisse les politiques et procédures à suivre ainsi que les mesures à prendre en cas de crises, de perturbations ou d'urgences. Le processus comprend des exercices d'entraînement au cours desquels des scénarios perturbateurs sont simulés.

I. Un processus est en place pour s'assurer que les ressources opérationnelles, humaines, technologiques et financières nécessaires sont budgétisées et disponibles en cas de crises, de perturbations ou d'urgences. Les ressources financières nécessaires au soutien de la résilience organisationnelle sont périodiquement analysées et communiquées au Conseil.

J. Un processus est en place pour examiner les crises, les perturbations et les situations d'urgence après leur survenance, en analysant les retours d'expérience et les leçons tirées, incluant l'intégration de ces enseignements dans la planification future de la résilience organisationnelle.

À propos de l'Institut des auditeurs internes

The Institute of Internal Auditors (IIA) est une association professionnelle internationale qui compte plus de 265 000 membres dans le monde et a décerné plus de 200 000 certifications Certified Internai Auditor (CIA®) dans le monde. Fondé 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, visitez le site theiia.org.

Droit d'auteur

Avril 2026

The Institute of Internal Auditors

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