NORME INTERNATIONALE

ISO/IEC 27001

Troisième édition
2022-10

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Numéro de référence
ISO/IEC 27001:2022(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ~~ISO~~. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets) ou dans la liste des déclarations de brevets reçues par l'IEC (voir https://patents.iec.ch).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27001:2013) qui a fait l'objet d'une révision technique. Elle incorpore également les Rectificatifs techniques ISO/IEC 27001:2013/Cor 1:2014 et ISO/IEC 27001:2013/Cor 2:2015.

Les principales modifications sont les suivantes :

— le texte a été aligné avec la structure harmonisée des normes de système de management et l'ISO/IEC 27002:2022.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/members.html et www.iec.ch/national-committees.

Introduction

0.1 Généralités

Le présent document a été élaboré pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l'information. L'adoption d'un système de management de la sécurité de l'information relève d'une décision stratégique de l'organisation. L'établissement et la mise en œuvre d'un système de management de la sécurité de l'information d'une organisation tiennent compte des besoins et des objectifs de l'organisation, des exigences de sécurité, des processus organisationnels mis en œuvre, ainsi que de la taille et de la structure de l'organisation. Tous ces facteurs d'influence sont appelés à évoluer dans le temps.

Le système de management de la sécurité de l'information préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate.

Il est important que le système de management de la sécurité de l'information fasse partie intégrante des processus et de la structure de management d'ensemble de l'organisation et que la sécurité de l'information soit prise en compte dans la conception des processus, des systèmes d'information et des mesures de sécurité. Il est prévu qu'un système de management de la sécurité de l'information évolue conformément aux besoins de l'organisation.

Le présent document peut être utilisé par les parties internes et externes pour évaluer la capacité de l'organisation à répondre à ses propres exigences en matière de sécurité de l'information.

L'ordre dans lequel les exigences sont présentées dans le présent document ne reflète pas leur importance ni l'ordre dans lequel elles doivent être mises en œuvre. Les éléments des listes sont énumérés uniquement à des fins de référence.

L'ISO/IEC 27000 décrit une vue d'ensemble et le vocabulaire des systèmes de management de la sécurité de l'information, en se référant à la famille des normes du système de management de la sécurité de l'information (incluant l'ISO/IEC 27003,[2] l'ISO/IEC 27004[3] et l'ISO/IEC 27005[4]) avec les termes et les définitions qui s'y rapportent.

0.2 Compatibilité avec d'autres systèmes de management

Le présent document applique la structure de haut niveau, les titres de paragraphe identiques, le texte, les termes communs et les définitions fondamentales définies dans l'Annexe SL des Directives ISO/IEC, Partie 1, Supplément ISO consolidé, et, par conséquent, est compatible avec les autres normes de systèmes de management qui se conforment à l'Annexe SL.

Cette approche commune définie dans l'Annexe SL sera utile aux organisations qui choisissent de mettre en œuvre un système de management unique pour répondre aux exigences de deux ou plusieurs normes de systèmes de management.

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

1 Domaine d'application

Le présent document spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. Le présent document comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation. Les exigences fixées dans le présent document sont génériques et prévues pour s'appliquer à toute organisation, quels que soient son type, sa taille et sa nature. Il n'est pas admis qu'une organisation s'affranchisse de l'une des exigences spécifiées aux Articles 4 à 10 lorsqu'elle revendique la conformité au présent document.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO/IEC 27000 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

4 Contexte de l'organisation

4.1 Compréhension de l'organisation et de son contexte

L'organisation doit déterminer les enjeux externes et internes pertinents compte tenu de sa mission et qui ont une incidence sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son système de management de la sécurité de l'information.

NOTE Déterminer ces enjeux revient à établir le contexte externe et interne de l'organisation étudiée dans le paragraphe 5.4.1 de l'ISO 31000:2018[5].

4.2 Compréhension des besoins et attentes des parties intéressées

L'organisation doit déterminer :

a) les parties intéressées qui sont concernées par le système de management de la sécurité de l'information ;

b) les exigences pertinentes de ces parties intéressées ;

c) lesquelles de ces exigences seront traitées par le biais du système de management de la sécurité de l'information.

NOTE Les exigences des parties intéressées peuvent inclure des exigences légales et réglementaires et des obligations contractuelles.

4.3 Détermination du domaine d'application du système de management de la sécurité de l'information

Pour établir le domaine d'application du système de management de la sécurité de l'information, l'organisation doit en déterminer les limites et l'applicabilité.

Lorsque l'organisation établit ce domaine d'application, elle doit prendre en compte :

a) les enjeux externes et internes auxquels il est fait référence en 4.1 ;

b) les exigences auxquelles il est fait référence en 4.2 ;

c) les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations.

Le domaine d'application doit être disponible sous la forme d'une information documentée.

4.4 Système de management de la sécurité de l'information

L'organisation doit établir, mettre en œuvre, tenir à jour et améliorer en continu un système de management de la sécurité de l'information, y compris les processus nécessaires et leurs interactions, en accord avec les exigences du présent document.

5 Leadership

5.1 Leadership et engagement

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management de la sécurité de l'information en :

a) s'assurant qu'une politique et des objectifs sont établis en matière de sécurité de l'information et qu'ils sont compatibles avec l'orientation stratégique de l'organisation ;

b) s'assurant que les exigences liées au système de management de la sécurité de l'information sont intégrées aux processus métiers de l'organisation ;

c) s'assurant que les ressources nécessaires pour le système de management de la sécurité de l'information sont disponibles ;

d) communiquant sur l'importance de disposer d'un management de la sécurité de l'information efficace et de se conformer aux exigences du système de management de la sécurité de l'information ;

e) s'assurant que le système de management de la sécurité de l'information produit le(s) résultat(s) escompté(s) ;

f) orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du système de management de la sécurité de l'information ;

g) promouvant l'amélioration continue ; et

h) aidant les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités.

NOTE Dans le présent document, il est possible d'interpréter le terme « métier » au sens large, c'est-à-dire comme se référant aux activités liées à la finalité de l'organisation.

5.2 Politique

La direction doit établir une politique de sécurité de l'information qui :

a) est appropriée à la mission de l'organisation ;

b) inclut des objectifs de sécurité de l'information (voir 6.2) ou fournit un cadre pour l'établissement de ces objectifs ;

c) inclut l'engagement de satisfaire aux exigences applicables en matière de sécurité de l'information ;

d) inclut l'engagement d'œuvrer pour l'amélioration continue du système de management de la sécurité de l'information.

La politique de sécurité de l'information doit :

e) être disponible sous forme d'information documentée ;

f) être communiquée au sein de l'organisation ;

g) être mise à la disposition des parties intéressées, le cas échéant.

5.3 Rôles, responsabilités et autorités au sein de l'organisation

La direction doit s'assurer que les responsabilités et autorités des rôles concernés par la sécurité de l'information sont attribuées et communiquées au sein de l'organisation.

La direction doit attribuer la responsabilité et l'autorité pour :

a) s'assurer que le système de management de la sécurité de l'information est conforme aux exigences du présent document ;

b) rendre compte à la direction des performances du système de management de la sécurité de l'information.

NOTE La direction peut également attribuer des responsabilités et autorités pour rendre compte des performances du système de management de la sécurité de l'information au sein de l'organisation.

6 Planification

6.1 Actions à mettre en œuvre face aux risques et opportunités

6.1.1 Généralités

Lorsqu'il conçoit son système de management de la sécurité de l'information, l'organisation doit tenir compte des enjeux de 4.1 et des exigences de 4.2, et déterminer les risques et opportunités qui nécessitent d'être abordés pour :

a) s'assurer que le système de management de la sécurité de l'information peut atteindre le(s) résultat(s) escompté(s) ;

b) empêcher ou limiter les effets indésirables ; et

c) obtenir une démarche d'amélioration continue.

L'organisation doit planifier :

d) les actions menées pour traiter ces risques et opportunités ; et

e) la manière :

1) d'intégrer et de mettre en œuvre les actions au sein des processus du système de management de la sécurité de l'information ; et

2) d'évaluer l'efficacité de ces actions.

6.1.2 Appréciation des risques de sécurité de l'information

L'organisation doit définir et appliquer un processus d'appréciation des risques de sécurité de l'information qui :

a) établit et tient à jour les critères de risque de sécurité de l'information incluant :

1) les critères d'acceptation des risques ;

2) les critères de réalisation des appréciations des risques de sécurité de l'information ;

b) s'assure que la répétition de ces appréciations des risques produit des résultats cohérents, valides et comparables ;

c) identifie les risques de sécurité de l'information :

1) applique le processus d'appréciation des risques de sécurité de l'information pour identifier les risques de perte de confidentialité, d'intégrité et de disponibilité des informations entrant dans le domaine d'application du système de management de la sécurité de l'information ; et

2) identifie les propriétaires des risques ;

d) analyse les risques de sécurité de l'information :

1) apprécie les conséquences potentielles dans le cas où les risques identifiés en 6.1.2 c) 1) se concrétisaient ;

2) procède à une évaluation réaliste de la vraisemblance d'apparition des risques identifiés en 6.1.2 c) 1) ; et

3) détermine les niveaux des risques ;

e) évalue les risques de sécurité de l'information :

1) compare les résultats d'analyse des risques avec les critères de risque déterminés en 6.1.2 a) ; et

2) priorise les risques analysés pour le traitement des risques.

L'organisation doit conserver des informations documentées sur le processus d'appréciation des risques de sécurité de l'information.

6.1.3 Traitement des risques de sécurité de l'information

L'organisation doit définir et appliquer un processus de traitement des risques de sécurité de l'information pour :

a) choisir les options de traitement des risques appropriées, en tenant compte des résultats de l'appréciation des risques ;

b) déterminer toutes les mesures de sécurité nécessaires à la mise en œuvre de(s) (l')option(s) de traitement des risques de sécurité de l'information choisie(s) ;

NOTE 1 Les organisations peuvent concevoir ces mesures de sécurité, le cas échéant, ou bien les identifier à partir de n'importe quelle source.

c) comparer les mesures de sécurité déterminées ci-dessus en 6.1.3 b) avec celles de l'Annexe A et vérifier qu'aucune mesure de sécurité nécessaire n'a été omise ;

NOTE 2 L'Annexe A comporte une liste de possibles mesures de sécurité de l'information. Les utilisateurs du présent document sont invités à se reporter à l'Annexe A pour s'assurer qu'aucune mesure de sécurité de l'information nécessaire n'a été négligée.

NOTE 3 Les mesures de sécurité de l'information énumérées dans l'Annexe A ne sont pas exhaustives et des mesures de sécurité de l'information additionnelles peuvent être incluses si nécessaires.

d) produire une déclaration d'applicabilité contenant :

— les mesures de sécurité nécessaires (voir 6.1.3 b) et c)) ;

— la justification de leur insertion ;

— si les mesures de sécurité nécessaires sont mises en œuvre ou non ; et

— la justification de l'exclusion de mesures de sécurité de l'Annexe A ;

e) élaborer un plan de traitement des risques de sécurité de l'information ; et

f) obtenir des propriétaires des risques l'approbation du plan de traitement des risques et l'acceptation des risques résiduels de sécurité de l'information.

L'organisation doit conserver des informations documentées sur le processus de traitement des risques de sécurité de l'information.

NOTE 4 L'appréciation des risques de sécurité de l'information et le processus de traitement figurant dans le présent document s'alignent sur les principes et les lignes directrices générales fournies dans l'ISO 31000[5].

6.2 Objectifs de sécurité de l'information et plans pour les atteindre

L'organisation doit établir, aux fonctions et niveaux concernés, des objectifs de sécurité de l'information.

Les objectifs de sécurité de l'information doivent :

a) être cohérents avec la politique de sécurité de l'information ;

b) être mesurables (si possible) ;

c) tenir compte des exigences applicables à la sécurité de l'information, et des résultats de l'appréciation et du traitement des risques ;

d) être surveillés ;

e) être communiqués ;

f) être mis à jour comme approprié ;

g) être tenus à jour sous la forme d'une information documentée.

L'organisation doit conserver des informations documentées sur les objectifs de sécurité de l'information.

Lorsqu'il planifie la façon d'atteindre ses objectifs de sécurité de l'information, l'organisation doit déterminer :

h) ce qui sera fait ;

i) quelles ressources seront requises ;

j) qui sera responsable ;

k) les échéances ; et

l) la façon dont les résultats seront évalués.

6.3 Planification des modifications

Lorsque l'organisation détermine qu'il est nécessaire de modifier le système de management de la sécurité de l'information, les modifications doivent être réalisées de façon planifiée.

7 Supports

7.1 Ressources

L'organisation doit identifier et fournir les ressources nécessaires à l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue du système de management de la sécurité de l'information.

7.2 Compétences

L'organisation doit :

a) déterminer les compétences nécessaires de la ou des personnes effectuant, sous son contrôle, un travail qui a une incidence sur les performances de la sécurité de l'information ;

b) s'assurer que ces personnes sont compétentes sur la base d'une formation initiale, d'une formation professionnelle ou d'une expérience appropriée ;

c) le cas échéant, mener des actions pour acquérir les compétences nécessaires et évaluer l'efficacité des actions entreprises ; et

d) conserver des informations documentées appropriées comme preuves desdites compétences.

NOTE Les actions envisageables peuvent notamment inclure la formation, l'encadrement ou la réaffectation du personnel actuellement employé ou le recrutement, direct ou en sous-traitance, de personnes compétentes.

7.3 Sensibilisation

Les personnes effectuant un travail sous le contrôle de l'organisation doivent :

a) être sensibilisées à la politique de sécurité de l'information ;

b) avoir conscience de leur contribution à l'efficacité du système de management de la sécurité de l'information, y compris aux effets positifs d'une amélioration des performances de la sécurité de l'information ; et

c) avoir conscience des implications de toute non-conformité aux exigences requises par le système de management de la sécurité de l'information.

7.4 Communication

L'organisation doit déterminer les besoins de communication interne et externe pertinents pour le système de management de la sécurité de l'information, et notamment :

a) sur quels sujets communiquer ;

b) quand communiquer ;

c) avec qui communiquer ;

d) comment communiquer.

7.5 Informations documentées

7.5.1 Généralités

Le système de management de la sécurité de l'information de l'organisation doit inclure :

a) les informations documentées exigées par le présent document ; et

b) les informations documentées que l'organisation juge nécessaires à l'efficacité du système de management de la sécurité de l'information.

NOTE L'étendue des informations documentées dans le cadre d'un système de management de la sécurité de l'information peut différer selon l'organisation en fonction de :

1) la taille de l'organisation, ses domaines d'activité et ses processus, produits et services ;

2) la complexité des processus et de leurs interactions ; et

3) la compétence des personnes.

7.5.2 Création et mise à jour

Quand il crée et met à jour ses informations documentées, l'organisation doit s'assurer que sont appropriés :

a) l'identification et la description (par exemple titre, date, auteur, numéro de référence) ;

b) le format (par exemple langue, version logicielle, graphiques) et le support (par exemple, papier, électronique) ; et

c) la revue et l'approbation du caractère adapté et adéquat des informations.

7.5.3 Contrôle des informations documentées

Les informations documentées exigées par le système de management de la sécurité de l'information et par le présent document doivent être contrôlées pour s'assurer :

a) qu'elles sont disponibles et conviennent à l'utilisation, où et quand elles sont nécessaires ; et

b) qu'elles sont convenablement protégées (par exemple contre la perte de confidentialité, l'utilisation inappropriée ou la perte d'intégrité).

Pour contrôler les informations documentées, l'organisation doit mettre en œuvre les activités suivantes, quand elles sont applicables :

c) distribution, accès, récupération et utilisation ;

d) stockage et conservation, y compris préservation de la lisibilité ;

e) contrôle des modifications (par exemple, contrôle des versions) ; et

f) durée de conservation et suppression.

Les informations documentées d'origine externe que l'organisation juge nécessaires à la planification et au fonctionnement du système de management de la sécurité de l'information doivent être identifiées comme il convient et contrôlées.

NOTE L'accès peut impliquer une décision relative à l'autorisation de consulter les informations documentées uniquement, ou l'autorisation et l'autorité de consulter et modifier les informations documentées, etc.

8 Fonctionnement

8.1 Planification et contrôle opérationnels

L'organisation doit planifier, mettre en œuvre et contrôler les processus nécessaires pour satisfaire aux exigences et réaliser les actions déterminées dans l'Article 6, en :

— établissant des critères pour ces processus ;

— mettant en œuvre le contrôle de ces processus conformément aux critères.

Les informations documentées doivent être disponibles dans une mesure suffisante pour avoir l'assurance que les processus ont été suivis comme prévu.

L'organisation doit contrôler les modifications prévues, analyser les conséquences des modifications imprévues et, si nécessaire, mener des actions pour limiter tout effet négatif.

L'organisation doit s'assurer que les processus, produits ou services fournis en externe et pertinents pour le système de management de la sécurité de l'information sont contrôlés.

8.2 Appréciation des risques de sécurité de l'information

L'organisation doit réaliser des appréciations des risques de sécurité de l'information à des intervalles planifiés ou quand des changements significatifs sont prévus ou ont lieu, en tenant compte des critères établis en 6.1.2 a).

L'organisation doit conserver des informations documentées sur les résultats des processus d'appréciation des risques de sécurité de l'information.

8.3 Traitement des risques de sécurité de l'information

L'organisation doit mettre en œuvre le plan de traitement des risques de sécurité de l'information.

L'organisation doit conserver des informations documentées sur les résultats du traitement des risques de sécurité de l'information.

9 Évaluation de la performance

9.1 Surveillance, mesurages, analyse et évaluation

L'organisation doit déterminer :

a) ce qu'il est nécessaire de surveiller et de mesurer, y compris les processus et les mesures de sécurité de l'information ;

b) les méthodes de surveillance, de mesurage, d'analyse et d'évaluation, selon les cas, pour assurer la validité des résultats. Il convient que les méthodes choisies donnent des résultats comparables et reproductibles pour être considérées comme valables ;

c) quand la surveillance et le mesurage doivent être effectués ;

d) qui doit effectuer la surveillance et les mesurages ;

e) quand les résultats de la surveillance et du mesurage doivent être analysés et évalués ;

f) qui doit analyser et évaluer ces résultats.

Des informations documentées doivent être disponibles comme preuve des résultats.

L'organisation doit évaluer les performances de sécurité de l'information, ainsi que l'efficacité du système de management de la sécurité de l'information.

9.2 Audit interne

9.2.1 Généralités

L'organisation doit réaliser des audits internes à des intervalles planifiés afin de recueillir des informations permettant de déterminer si le système de management de la sécurité de l'information :

a) est conforme :

   1) aux exigences propres de l'organisation concernant son système de management de la sécurité de l'information ;

   2) aux exigences du présent document ;

b) est efficacement mise en œuvre et maintenu.

9.2.2 Programme d'audit interne

L'organisation doit planifier, établir, mettre en œuvre et tenir à jour ou plusieurs programmes d'audit, couvrant notamment la fréquence, les méthodes, les responsabilités, les exigences de planification et les comptes rendus.

Lors de l'établissement du ou des programmes d'audit internes, l'organisation doit tenir compte de l'importance des processus concernés et des résultats des audits précédents.

L'organisation doit :

a) définir les critères d'audit et le périmètre de chaque audit ;

b) sélectionner des auditeurs et réaliser des audits qui assurent l'objectivité et l'impartialité du processus d'audit ;

c) veiller à ce que les résultats des audits soient communiqués à la direction concernée

Des informations documentées doivent être disponibles comme preuve de la mise en œuvre du ou des programmes d'audit et des résultats d'audit.

9.3 Revue de direction

9.3.1 Généralités

À des intervalles planifiés, la direction doit procéder à la revue du système de management de la sécurité de l'information mis en place par l'organisation, afin de s'assurer qu'il est toujours approprié, adapté et efficace.

9.3.2 Éléments d'entrée de la revue de direction

La revue de direction doit prendre en considération :

a) l'état d'avancement des actions décidées lors des revues de direction précédentes ;

b) les modifications des enjeux externes et internes pertinents pour le système de management de la sécurité de l'information ;

c) les modifications des besoins et attentes des parties intéressées, pertinentes pour le système de management de la sécurité de l'information ;

d) les retours sur les performances de sécurité de l'information, y compris les tendances concernant :

   1) les non-conformités et les actions correctives ;

   2) les résultats de la surveillance et du mesurage ;

   3) les résultats des audits ;

   4) la réalisation des objectifs en matière de sécurité de l'information ;

e) les retours d'information des parties intéressées ;

f) les résultats de l'appréciation des risques et l'état d'avancement du plan de traitement des risques ;

g) des opportunités d'amélioration continue.

9.3.3 Résultats des revues de direction

Les résultats de la revue de direction doivent inclure les décisions relatives aux opportunités d'amélioration continue et aux éventuels changements à apporter au système de management de la sécurité de l'information.

Des informations documentées doivent être disponibles comme preuve des résultats des revues de direction.

10 Amélioration

10.1 Amélioration continue

L'organisation doit continuellement améliorer la pertinence, l'adéquation et l'efficacité du système de management de la sécurité de l'information.

10.2 Non-conformité et action corrective

Lorsqu'une non-conformité se produit, l'organisation doit :

a) réagir à la non-conformité, et le cas échéant :

   1) agir pour la contrôler et la corriger ;

   2) faire face aux conséquences ;

b) évaluer s'il est nécessaire de mener une action pour éliminer les causes de la non-conformité, de sorte qu'elle ne se reproduise plus, ou qu'elle ne se produise pas ailleurs, en :

   1) passant en revue la non-conformité ;

   2) déterminant les causes de non-conformité ; et

   3) recherchant si des non-conformités similaires existent ou pourraient éventuellement se produire ;

c) mettant en œuvre toute action nécessaire ;

d) passant en revue l'efficacité de toute action corrective mise en œuvre ; et

e) modifiant, si nécessaire, le système de management de sécurité de l'information.

Les actions correctives doivent être appropriées aux conséquences des non-conformités rencontrées.

Des informations documentées doivent être disponibles comme preuve :

f) de la nature des non-conformités et de toute action menée ultérieurement ;

g) des résultats de toute action corrective.

Annexe A
(normative)

Référencement des mesures de sécurité de l'information

Les mesures de sécurité de l'information énumérées dans le Tableau A.1 découlent directement de celles qui sont répertoriées dans la norme ISO/IEC 27002:2022,[1] Articles 5 à 8, avec lesquelles elles sont alignées, et doivent être utilisées dans le contexte du paragraphe 6.1.3.

Tableau A.1 — Mesures de sécurité de l'information

5	**Mesures de sécurité organisationnelles**	
5.1	Politiques de sécurité de l'information	**Mesure de sécurité** Une politique de sécurité de l'information et des politiques spécifiques à une thématique doivent être définies, approuvées par la direction, publiées, communiquées et demandée en confirmation au personnel et aux parties intéressées concernés, ainsi que révisées à intervalles planifiés et si des changements significatifs ont lieu.
5.2	Fonctions et responsabilités liées à la sécurité de l'information	**Mesure de sécurité** Les fonctions et responsabilités liées à la sécurité de l'information doivent être définies et attribuées selon les besoins de l'organisation.
5.3	Séparation des tâches	**Mesure de sécurité** Les tâches et les domaines de responsabilité incompatibles doivent être séparés.
5.4	Responsabilités de la direction	**Mesure de sécurité** La direction doit demander à tout le personnel d'appliquer les mesures de sécurité de l'information conformément à la politique de sécurité de l'information, aux politiques spécifiques à une thématique et aux procédures établies de l'organisation.
5.5	Contacts avec les autorités	**Mesure de sécurité** L'organisation doit établir et maintenir le contact avec les autorités appropriées.
5.6	Contacts avec des groupes d'intérêt spécifiques	**Mesure de sécurité** L'organisation doit établir et maintenir des contacts avec des groupes d'intérêt spécifiques ou autres forums spécialisés sur la sécurité et associations professionnelles.
5.7	Renseignement sur les menaces	**Mesure de sécurité** Les informations relatives aux menaces de sécurité de l'information doivent être collectées et analysées pour produire les renseignements sur les menaces.
5.8	Sécurité de l'information dans la gestion de projet	**Mesure de sécurité** La sécurité de l'information doit être intégrée à la gestion de projet.
5.9	Inventaire des informations et autres actifs associés	**Mesure de sécurité** Un inventaire des informations et des autres actifs associés, y compris leurs propriétaires, doit être élaboré et tenu à jour.

Tableau A.1 *(suite)*

5.10	Utilisation correcte des informations et autres actifs associés	**Mesure de sécurité** Des règles d'utilisation correcte et des procédures de traitement des informations et autres actifs associés doivent être identifiées, documentées et mises en œuvre.
5.11	Restitution des actifs	**Mesure de sécurité** Le personnel et les autres parties intéressées, selon le cas, doivent restituer tous les actifs de l'organisation qui sont en leur possession au moment du changement ou de la fin de leur emploi, contrat ou accord.
5.12	Classification des informations	**Mesure de sécurité** Les informations doivent être classifiées conformément aux besoins de sécurité de l'information de l'organisation, sur la base des exigences de confidentialité, d'intégrité, de disponibilité, et des exigences importantes des parties intéressées.
5.13	Marquage des informations	**Mesure de sécurité** Un ensemble approprié de procédures pour le marquage des informations doit être élaboré et mis en œuvre conformément au schéma de classification des informations adopté par l'organisation.
5.14	Transfert des informations	**Mesure de sécurité** Des règles, procédures ou accords sur le transfert des informations doivent être mis en place pour tous les types de moyens de transfert au sein de l'organisation et entre l'organisation et des tierces parties.
5.15	Contrôle d'accès	**Mesure de sécurité** Des règles visant à contrôler l'accès physiques et logique aux informations et autres actifs associés doivent être définies et mises en œuvre, en fonction des exigences métier et de sécurité de l'information.
5.16	Gestion des identités	**Mesure de sécurité** Le cycle de vie complet des identités doit être géré.
5.17	Informations d'authentification	**Mesure de sécurité** L'attribution et la gestion des informations d'authentification doivent être contrôlées par un processus de gestion, incluant des recommandations au personnel sur l'utilisation appropriée des informations d'authentification.
5.18	Droits d'accès	**Mesure de sécurité** Les droits d'accès aux informations et autres actifs associés doivent être pourvus, révisés, modifiés et supprimés conformément à la politique spécifique à la thématique du contrôle d'accès et aux règles de contrôle d'accès de l'organisation.
5.19	Sécurité de l'information dans les relations avec les fournisseurs	**Mesure de sécurité** Des processus et procédures pour gérer les risques de sécurité de l'information qui sont associés à l'utilisation des produits ou services du fournisseur doivent être définis et mis en œuvre.
5.20	La sécurité de l'information dans les accords conclus avec les fournisseurs	**Mesure de sécurité** Les exigences de sécurité de l'information appropriées doivent être mises en place et convenues avec chaque fournisseur, selon le type de relation avec le fournisseur.

Tableau A.1 *(suite)*

5.21	Gestion de la sécurité de l'information dans la chaîne d'approvisionnement des technologies de l'information et de la communication (TIC)	**Mesure de sécurité** Des processus et procédures pour gérer les risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et services TIC doivent être définis et mis en œuvre.
5.22	Surveillance, révision et gestion des changements des services fournisseurs	**Mesure de sécurité** L'organisation doit procéder régulièrement à la surveillance, à la révision, à l'évaluation et à la gestion des changements des pratiques de sécurité de l'information du fournisseur et de prestation de services.
5.23	Sécurité de l'information dans l'utilisation de services en nuage	**Mesure de sécurité** Les processus d'acquisition, d'utilisation, de gestion et de cessation des services en nuage doivent être établis conformément aux exigences de sécurité de l'information de l'organisation.
5.24	Planification et préparation de la gestion des incidents de sécurité de l'information	**Mesure de sécurité** L'organisation doit planifier et préparer la gestion des incidents de sécurité de l'information en procédant à la définition, à l'établissement et à la communication des processus, fonctions et responsabilités liés à la gestion des incidents de sécurité de l'information.
5.25	Évaluation des événements de sécurité de l'information et prise de décision	**Mesure de sécurité** L'organisation doit évaluer les événements de sécurité de l'information et décider s'ils doivent être catégorisés comme des incidents de sécurité de l'information.
5.26	Réponse aux incidents de sécurité de l'information	**Mesure de sécurité** La réponse aux incidents de sécurité de l'information doit être conforme aux procédures documentées.
5.27	Tirer des enseignements des incidents de sécurité de l'information	**Mesure de sécurité** Les connaissances acquises à partir des incidents de sécurité de l'information doivent être utilisées pour renforcer et améliorer les mesures de sécurité de l'information.
5.28	Collecte de preuves	**Mesure de sécurité** L'organisation doit établir et mettre en œuvre des procédures pour l'identification, la collecte, l'acquisition et la préservation des preuves relatives aux événements de sécurité de l'information.
5.29	Sécurité de l'information pendant une perturbation	**Mesure de sécurité** L'organisation doit planifier comment maintenir la sécurité de l'information au niveau approprié pendant une perturbation.
5.30	Préparation des TIC pour la continuité d'activité	**Mesure de sécurité** La préparation des TIC doit être planifiée, mise en œuvre, maintenue et testée en se basant sur les objectifs de continuité d'activité et des exigences de continuité des TIC.
5.31	Exigences légales, statutaires, réglementaires et contractuelles	**Mesure de sécurité** Les exigences légales, statutaires, réglementaires et contractuelles pertinentes pour la sécurité de l'information, ainsi que l'approche de l'organisation pour respecter ces exigences, doivent être identifiées, documentées et tenues à jour.
5.32	Droits de propriété intellectuelle	**Mesure de sécurité** L'organisation doit mettre en œuvre les procédures appropriées pour protéger les droits de propriété intellectuelle.

Tableau A.1 *(suite)*

5.33	Protection des enregistrements	**Mesure de sécurité** Les enregistrements doivent être protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées.
5.34	Protection de la vie privée et des données à caractère personnel (DCP)	**Mesure de sécurité** L'organisation doit identifier et respecter les exigences relatives à la protection de la vie privée et des DCP conformément aux lois, réglementations et exigences contractuelles applicables.
5.35	Révision indépendante de la sécurité de l'information	**Mesure de sécurité** L'approche de l'organisation pour gérer la sécurité de l'information et sa mise en œuvre, y compris les personnes, les processus et les technologies, doit être révisée de manière indépendante à intervalles planifiés, ou lorsque des changements significatifs se produisent.
5.36	Conformité aux politiques, règles et normes de sécurité de l'information	**Mesure de sécurité** La conformité à la politique de sécurité de l'information, aux politiques spécifiques à une thématique, aux règles et aux normes de l'organisation doit être régulièrement vérifiée.
5.37	Procédures d'exploitation documentées	**Mesure de sécurité** Les procédures d'exploitation des moyens de traitement de l'information doivent être documentées et mises à disposition du personnel qui en a besoin.
6	**Mesures de sécurité applicables aux personnes**	
6.1	Sélection des candidats	**Mesure de sécurité** Les vérifications des références de tous les candidats à l'embauche doivent être réalisées avant qu'ils n'intègrent l'organisation puis de façon continue en tenant compte des lois, des réglementations et de l'éthique applicables, et doivent être proportionnelles aux exigences métier, à la classification des informations auxquelles ils auront accès et aux risques identifiés.
6.2	Termes et conditions du contrat de travail	**Mesure de sécurité** Les contrats de travail doivent indiquer les responsabilités du personnel et de l'organisation en matière de sécurité de l'information.
6.3	Sensibilisation, enseignement et formation en sécurité de l'information	**Mesure de sécurité** Le personnel de l'organisation et les parties intéressées pertinentes doivent recevoir une sensibilisation, un enseignement et des formations en sécurité de l'information appropriés, ainsi que des mises à jour régulières de la politique de sécurité de l'information, des politiques spécifiques à une thématique et des procédures de l'organisation pertinentes à leur fonction.
6.4	Processus disciplinaire	**Mesure de sécurité** Un processus disciplinaire permettant de prendre des mesures à l'encontre du personnel et d'autres parties intéressées qui ont commis une violation de la politique de sécurité de l'information doit être formalisé et communiqué.
6.5	Responsabilités après la fin ou le changement d'un emploi	**Mesure de sécurité** Les responsabilités et les obligations relatives à la sécurité de l'information qui restent valables après la fin ou le changement d'un emploi doivent être définies, appliquées et communiquées au personnel et autres parties intéressées pertinentes.

Tableau A.1 *(suite)*

6.6	Accords de confidentialité ou de non-divulgation	**Mesure de sécurité** Des accords de confidentialité ou de non-divulgation, représentant les besoins de l'organisation relatifs à la protection des informations, doivent être identifiés, documentés, régulièrement révisés et signés.
6.7	Travail à distance	**Mesure de sécurité** Des mesures de sécurité doivent être mises en œuvre lorsque le personnel travaille à distance, pour protéger les informations accessibles, traitées ou stockées en dehors des locaux de l'organisation.
6.8	Déclaration des événements de sécurité de l'information	**Mesure de sécurité** L'organisation doit fournir un mécanisme au personnel pour déclarer rapidement les événements de sécurité de l'information observés ou suspectés, à travers des canaux appropriés.
7	**Mesures de sécurité physique**	
7.1	Périmètres de sécurité physique	**Mesure de sécurité** Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones qui contiennent les informations et autres actifs associés.
7.2	Les entrées physiques	**Mesure de sécurité** Les zones sécurisées doivent être protégées par des mesures de sécurité des accès et des points d'accès appropriés.
7.3	Sécurisation des bureaux, des salles et des installations	**Mesure de sécurité** Des mesures de sécurité physique pour les bureaux, les salles et les installations doivent être conçues et mises en œuvre.
7.4	Surveillance de la sécurité physique	**Mesure de sécurité** Les locaux doivent être continuellement surveillés pour empêcher l'accès physique non autorisé.
7.5	Protection contre les menaces physiques et environnementales	**Mesure de sécurité** Une protection contre les menaces physiques et environnementales, telles que les catastrophes naturelles et autres menaces physiques, intentionnelles ou non intentionnelles, impactant l'infrastructure, doit être conçue et mise en œuvre.
7.6	Travail dans les zones sécurisées	**Mesure de sécurité** Des mesures de sécurité pour le travail dans les zones sécurisées doivent être conçues et mises en œuvre.
7.7	Bureau propre et écran vide	**Mesure de sécurité** Des règles du bureau vide, dégagé des documents papier et des supports de stockage amovibles, et des règles de l'écran vide pour les moyens de traitement de l'information, doivent être définies et appliquées de manière appropriée.
7.8	Emplacement et protection du matériel	**Mesure de sécurité** Un emplacement sécurisé pour le matériel doit être choisi et protégé.
7.9	Sécurité des actifs hors des locaux	**Mesure de sécurité** Les actifs hors du site doivent être protégés.
7.10	Supports de stockage	**Mesure de sécurité** Les supports de stockage doivent être gérés tout au long de leur cycle de vie d'acquisition, d'utilisation, de transport et de mise au rebut, conformément au schéma de classification et aux exigences de traitement de l'organisation.

Tableau A.1 *(suite)*

7.11	Services supports	**Mesure de sécurité** Les moyens de traitement de l'information doivent être protégés contre les coupures de courant et autres perturbations causées par des défaillances des services supports.
7.12	Sécurité du câblage	**Mesure de sécurité** Les câbles électriques, transportant des données ou supportant les services d'information, doivent être protégés contre des interceptions, interférences ou dommages.
7.13	Maintenance du matériel	**Mesure de sécurité** Le matériel doit être entretenu correctement pour assurer la disponibilité, l'intégrité et la confidentialité de l'information.
7.14	Élimination ou recyclage sécurisé(e) du matériel	**Mesure de sécurité** Les éléments du matériel contenant des supports de stockage doivent être vérifiés pour s'assurer que toute donnée sensible et que tout logiciel sous licence ont été supprimés ou écrasés de façon sécurisée, avant son élimination ou sa réutilisation.
8	**Mesures de sécurité technologiques**	
8.1	Terminaux finaux des utilisateurs	**Mesure de sécurité** Les informations stockées, traitées ou accessibles via les terminaux finaux des utilisateurs, doivent être protégées.
8.2	Droits d'accès privilégiés	**Mesure de sécurité** L'attribution et l'utilisation des droits d'accès privilégiés doivent être limitées et gérées.
8.3	Restriction d'accès aux informations	**Mesure de sécurité** L'accès aux informations et autres actifs associés doit être restreint conformément à la politique spécifique à la thématique du contrôle d'accès qui a été établie.
8.4	Accès aux codes source	**Mesure de sécurité** L'accès en lecture et en écriture au code source, aux outils de développement et aux bibliothèques de logiciels doit être géré de manière appropriée.
8.5	Authentification sécurisée	**Mesure de sécurité** Des technologies et procédures d'authentification sécurisées doivent être mises en œuvre sur la base des restrictions d'accès aux informations et de la politique spécifique à la thématique du contrôle d'accès.
8.6	Dimensionnement	**Mesure de sécurité** L'utilisation des ressources doit être surveillée et ajustée selon les besoins de dimensionnement actuels et prévus.
8.7	Protection contre les programmes malveillants (*malware*)	**Mesure de sécurité** Une protection contre les programmes malveillants doit être mise en œuvre et renforcée par une sensibilisation appropriée des utilisateurs.
8.8	Gestion des vulnérabilités techniques	**Mesure de sécurité** Des informations sur les vulnérabilités techniques des systèmes d'information utilisés doivent être obtenues, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et des mesures appropriées doivent être prises.

Tableau A.1 *(suite)*

8.9	Gestion des configurations	**Mesure de sécurité** Les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux, doivent être définies, documentées, mises en œuvre, surveillées et révisées.
8.10	Suppression des informations	**Mesure de sécurité** Les informations stockées dans les systèmes d'information, les terminaux ou tout autre support de stockage doivent être supprimées lorsqu'elles ne sont plus nécessaires.
8.11	Masquage des données	**Mesure de sécurité** Le masquage des données doit être utilisé conformément à la politique spécifique à la thématique du contrôle d'accès de l'organisation et d'autres politiques spécifiques à une thématique associées, ainsi qu'aux exigences métier, tout en prenant en compte la législation applicable.
8.12	Prévention de la fuite de données	**Mesure de sécurité** Des mesures de prévention de la fuite de données doivent être appliquées aux systèmes, aux réseaux et à tous les autres terminaux qui traitent, stockent ou transmettent des informations sensibles.
8.13	Sauvegarde des informations	**Mesure de sécurité** Des copies de sauvegarde de l'information, des logiciels et des systèmes doivent être conservées et testées régulièrement selon la politique spécifique à la thématique de la sauvegarde qui a été convenue.
8.14	Redondance des moyens de traitement de l'information	**Mesure de sécurité** Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.
8.15	Journalisation	**Mesure de sécurité** Des journaux qui enregistrent les activités, les exceptions, les pannes et autres événements pertinents doivent être générés, conservés, protégés et analysés.
8.16	Activités de surveillance	**Mesure de sécurité** Les réseaux, systèmes et applications doivent être surveillés pour détecter les comportements anormaux et des mesures appropriées doivent être prises pour évaluer les éventuels incidents de sécurité de l'information.
8.17	Synchronisation des horloges	**Mesure de sécurité** Les horloges des systèmes de traitement de l'information utilisés par l'organisation doivent être synchronisées avec des sources de temps approuvées.
8.18	Utilisation de programmes utilitaires à privilèges	**Mesure de sécurité** L'utilisation des programmes utilitaires ayant la capacité de contourner les mesures de sécurité des systèmes ou des applications doit être limitée et contrôlée étroitement.
8.19	Installation de logiciels sur des systèmes opérationnels	**Mesure de sécurité** Des procédures et des mesures doivent être mises en œuvre pour gérer de manière sécurisée l'installation de logiciels sur les systèmes opérationnels.

Tableau A.1 *(suite)*

8.20	Sécurité des réseaux	**Mesure de sécurité** Les réseaux et les terminaux réseau doivent être sécurisés, gérés et contrôlés pour protéger les informations des systèmes et des applications.
8.21	Sécurité des services réseau	**Mesure de sécurité** Les mécanismes de sécurité, les niveaux de service et les exigences de services des services réseau doivent être identifiés, mis en œuvre et surveillés.
8.22	Cloisonnement des réseaux	**Mesure de sécurité** Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés dans les réseaux de l'organisation.
8.23	Filtrage web	**Mesure de sécurité** L'accès aux sites web externes doit être géré pour réduire l'exposition aux contenus malveillants.
8.24	Utilisation de la cryptographie	**Mesure de sécurité** Des règles pour l'utilisation efficace de la cryptographie, notamment la gestion des clés cryptographiques, doivent être définies et mises en œuvre.
8.25	Cycle de vie de développement sécurisé	**Mesure de sécurité** Des règles pour le développement sécurisé des logiciels et des systèmes doivent être définies et appliquées.
8.26	Exigences de sécurité des applications	**Mesure de sécurité** Les exigences de sécurité de l'information doivent être identifiées, spécifiées et approuvées lors du développement ou de l'acquisition d'applications.
8.27	Principes d'ingénierie et d'architecture des systèmes sécurisés	**Mesure de sécurité** Des principes d'ingénierie des systèmes sécurisés doivent être établis, documentés, tenus à jour et appliqués à toutes les activités de développement de systèmes d'information.
8.28	Codage sécurisé	**Mesure de sécurité** Des principes de codage sécurisé doivent être appliqués au développement de logiciels.
8.29	Tests de sécurité dans le développement et l'acceptation	**Mesure de sécurité** Des processus pour les tests de sécurité doivent être définis et mis en œuvre au cours du cycle de vie de développement.
8.30	Développement externalisé	**Mesure de sécurité** L'organisation doit diriger, contrôler et vérifier les activités relatives au développement externalisé des systèmes.
8.31	Séparation des environnements de développement, de test et opérationnels	**Mesure de sécurité** Les environnements de développement, de test et opérationnels doivent être séparés et sécurisés.
8.32	Gestion des changements	**Mesure de sécurité** Les changements apportés aux moyens de traitement de l'information et aux systèmes d'information doivent être soumis à des procédures de gestion des changements.
8.33	Informations de test	**Mesure de sécurité** Les informations de test doivent être sélectionnées, protégées et gérées de manière appropriée.

Tableau A.1 *(suite)*

8.34	Protection des systèmes d'information pendant les tests d'audit	**Mesure de sécurité** Les tests d'audit et autres activités d'assurance impliquant l'évaluation des systèmes opérationnels doivent être planifiés et convenus entre le testeur et le niveau approprié de la direction.

Bibliographie

[1] ISO/IEC 27002:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information*

[2] ISO/IEC 27003, *Technologies de l'information — Techniques de sécurité —Systèmes de management de la sécurité de l'information — Lignes directrices*

[3] ISO/IEC 27004, *Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation*

[4] ISO/IEC 27005, *Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information*

[5] ISO 31000:2018, *Management du risque — Lignes directrices*

ICS 03.100.70; 35.030

Prix basé sur 19 pages