Union internationale des télécommunications

# UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

# X.1054

(04/2021)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité de l'information et des réseaux – Gestion de la sécurité

## Sécurité de l'information, cybersécurité et protection de la vie privée – Gouvernance de la sécurité de l'information

Recommandation UIT-T X.1054

RECOMMANDATIONS UIT-T DE LA SÉRIE X

**RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ**

| | |
|---|---|
| RÉSEAUX PUBLICS DE DONNÉES | X.1–X.199 |
| INTERCONNEXION DES SYSTÈMES OUVERTS | X.200–X.299 |
| INTERFONCTIONNEMENT DES RÉSEAUX | X.300–X.399 |
| SYSTÈMES DE MESSAGERIE | X.400–X.499 |
| ANNUAIRE | X.500–X.599 |
| RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES | X.600–X.699 |
| GESTION OSI | X.700–X.799 |
| SÉCURITÉ | X.800–X.849 |
| APPLICATIONS OSI | X.850–X.899 |
| TRAITEMENT RÉPARTI OUVERT | X.900–X.999 |
| SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX | |
| Aspects généraux de la sécurité | X.1000–X.1029 |
| Sécurité des réseaux | X.1030–X.1049 |
| **Gestion de la sécurité** | **X.1050–X.1069** |
| Télébiométrie | X.1080–X.1099 |
| APPLICATIONS ET SERVICES SÉCURISÉS (1) | |
| Sécurité en multidiffusion | X.1100–X.1109 |
| Sécurité des réseaux domestiques | X.1110–X.1119 |
| Sécurité des télécommunications mobiles | X.1120–X.1139 |
| Sécurité de la toile (1) | X.1140–X.1149 |
| Sécurité des applications (1) | X.1150–X.1159 |
| Sécurité d'homologue à homologue | X.1160–X.1169 |
| Sécurité des identificateurs en réseau | X.1170–X.1179 |
| Sécurité de la télévision par réseau IP | X.1180–X.1199 |
| SÉCURITÉ DU CYBERESPACE | |
| Cybersécurité | X.1200–X.1229 |
| Lutte contre le spam | X.1230–X.1249 |
| Gestion des identités | X.1250–X.1279 |
| APPLICATIONS ET SERVICES SÉCURISÉS (2) | |
| Communications d'urgence | X.1300–X.1309 |
| Sécurité des réseaux de capteurs ubiquitaires | X.1310–X.1319 |
| Sécurité des réseaux électriques intelligents | X.1330–X.1339 |
| Courrier certifié | X.1340–X.1349 |
| Sécurité de l'Internet des objets (IoT) | X.1350–X.1369 |
| Sécurité des systèmes de transport intelligents | X.1370–X.1399 |
| Sécurité de la technologie des registres distribués (DLT) | X.1400–X.1429 |
| Sécurité des applications (2) | X.1450–X.1459 |
| Sécurité de la toile (2) | X.1470–X.1489 |
| ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ | |
| Aperçu général de la cybersécurité | X.1500–X.1519 |
| Échange concernant les vulnérabilités/les états | X.1520–X.1539 |
| Échange concernant les événements/les incidents/l'heuristique | X.1540–X.1549 |
| Échange de politiques | X.1550–X.1559 |
| Heuristique et demande d'informations | X.1560–X.1569 |
| Identification et découverte | X.1570–X.1579 |
| Échange garanti | X.1580–X.1589 |
| Cyberdéfense | X.1590–X.1599 |
| SÉCURITÉ DE L'INFORMATIQUE EN NUAGE | |
| Aperçu de la sécurité de l'informatique en nuage | X.1600–X.1601 |
| Conception de la sécurité de l'informatique en nuage | X.1602–X.1639 |
| Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage | X.1640–X.1659 |
| Mise en œuvre de la sécurité de l'informatique en nuage | X.1660–X.1679 |
| Sécurité de l'informatique en nuage (autres) | X.1680–X.1699 |
| COMMUNICATIONS QUANTIQUES | |
| Terminologie | X.1700–X.1701 |
| Générateur quantique de nombres aléatoires | X.1702–X.1709 |
| Cadre de sécurité pour les réseaux QKDN | X.1710–X.1711 |
| Conception de la sécurité pour les réseaux QKDN | X.1712–X.1719 |
| Techniques de sécurité pour les réseaux QKDN | X.1720–X.1729 |
| SÉCURITÉ DES DONNÉES | |
| Sécurité des mégadonnées | X.1750–X.1759 |
| Protection des données | X.1770–X.1789 |
| SÉCURITÉ DES IMT-2020 | X.1800–X.1819 |

*Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.*

**NORME INTERNATIONALE ISO/CEI 27014**
**RECOMMANDATION UIT-T X.1054**

# Sécurité de l'information, cybersécurité et protection de la vie privée
# Gouvernance de la sécurité de l'information


## Résumé

La Recommandation UIT-T X.1054 | Norme internationale ISO/CEI 27014 donne des orientations concernant la gouvernance de la sécurité de l'information.

La sécurité de l'information est une question fondamentale pour les organisations, qui a pris de l'importance en raison des progrès rapides accomplis dans les technologies et les méthodes d'attaque, ainsi que des pressions réglementaires connexes qui se sont accentuées.

La défaillance des contrôles de sécurité de l'information d'une organisation peut avoir de nombreuses conséquences négatives pour celle-ci et ses parties intéressées, y compris, sans toutefois s'y limiter, une détérioration du lien de confiance.

La gouvernance de la sécurité de l'information consiste à utiliser des ressources pour garantir l'application efficace des mesures ayant trait à la sécurité de l'information, et donne l'assurance:

- que les directives relatives à la sécurité de l'information seront respectées; et
- que l'organe directeur recevra des rapports fiables et pertinents sur les activités liées à la sécurité de l'information.

L'organe directeur prendrait des décisions plus éclairées concernant les objectifs stratégiques de l'organisation, puisqu'il disposerait de renseignements ayant trait à la sécurité de l'information pouvant influer sur ces objectifs. En outre, la concordance entre la stratégie en matière de sécurité de l'information et les objectifs généraux de l'entité serait assurée.

Les responsables et autres membres du personnel des organisations doivent comprendre:

- les exigences de gouvernance qui influent sur leur travail; et
- comment respecter les exigences de gouvernance qui leur imposent d'agir.



## Historique

| Édition | Recommandation | Approbation | Commission d'études | ID unique* |
|---|---|---|---|---|
| 1.0 | UIT-T X.1054 | 07-09-2012 | 17 | 11.1002/1000/11594 |
| 2.0 | UIT-T X.1054 | 30-04-2021 | 17 | 11.1002/1000/14248 |

## Mots clés

Sécurité de l'information, gouvernance de la sécurité de l'information, gestion de la sécurité de l'information, système de gestion de la sécurité de l'information (ISMS).


* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique de la Recommandation, par exemple http://handle.itu.int/11.1002/1000/11830-en.

## AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

## NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas des renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

**TABLE DES MATIÈRES**

**Introduction**

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale. L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes. L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT. Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) constituent ensemble le système spécialisé de la normalisation mondiale. Les organismes nationaux qui sont membres de l'ISO ou de la CEI participent à l'élaboration de Recommandations | Normes internationales dans le cadre de comités techniques établis par ces organisations dans des domaines techniques particuliers. Les comités techniques de l'ISO et de la CEI mènent des travaux en collaboration dans des domaines d'intérêt mutuel. D'autres organisations internationales, gouvernementales et non gouvernementales, participent également à ces travaux en liaison avec l'ISO et la CEI. Dans le domaine de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée, l'ISO et la CEI ont établi un comité technique mixte appelé ISO/CEI JTC 1.

La présente Recommandation | Norme internationale a été élaborée conformément aux règles figurant dans la deuxième partie des Directives ISO/CEI.

Le comité technique mixte a pour tâche essentielle d'élaborer la présente Recommandation | Norme internationale. Les projets de Recommandations | Normes internationales qu'il adopte sont soumis à l'approbation des organismes nationaux. Pour être publié à titre de norme internationale, un projet doit être approuvé par au moins 75% des organismes nationaux ayant exprimé leur voix.

Il convient de souligner que certains éléments de la présente Recommandation | Norme internationale peuvent être soumis à des droits de brevet. L'UIT, l'ISO ou la CEI ne sauraient être tenues responsables de l'indication de tout ou partie de ces droits.

La Recommandation UIT-T X.1054 | norme ISO/CEI 27014 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*, en collaboration avec la CE 17 de l'UIT-T.

**NORME INTERNATIONALE**
**RECOMMANDATION UIT-T**

# Sécurité de l'information, cybersécurité et protection de la vie privée – Gouvernance de la sécurité de l'information

## 1 Domaine d'application

La présente Recommandation | Norme internationale fournit des orientations concernant les concepts, objectifs et processus régissant la gouvernance de la sécurité de l'information, grâce auxquels les organisations peuvent mener à bien les processus "évaluer", "diriger", "surveiller" et "communiquer" liés à la sécurité de l'information établis en leur sein.

Le présent document s'adresse:

- à l'organe directeur et à la haute direction;
- aux responsables de l'évaluation, de la direction et de la surveillance d'un système de gestion de la sécurité de l'information (ISMS) basé sur la norme ISO/CEI 27001;
- aux responsables de la gestion de la sécurité de l'information qui s'effectue hors du cadre d'un système ISMS basé sur la norme ISO/CEI 27001, mais à l'intérieur du cadre de gouvernance.

La présente Recommandation | Norme internationale est applicable à toutes les organisations, quels que soient leur type et leur taille.

Toutes les références faites à un système ISMS dans le présent document désignent un système ISMS basé sur la norme ISO/CEI 27001.

La présente Recommandation | Norme internationale est axée sur les trois types d'organisation ISMS présentés dans l'Annexe B. Toutefois, elle peut également être utilisée par d'autres types d'organisation.

## 2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations UIT-T en vigueur.

– Norme ISO/CEI 27000 (en vigueur), *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

– Norme ISO/CEI 27001 (en vigueur), *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*.

## 3 Définitions

Aux fins de la présente Recommandation | Norme internationale, les termes et définitions figurant dans la norme ISO/CEI 27000 et les définitions ci-après s'appliquent.

L'ISO, la CEI et l'UIT tiennent à jour des bases de données terminologiques utilisées dans le domaine de la normalisation, qui sont accessibles aux liens suivants:

- Electropedia de la CEI: disponible à l'adresse http://www.electropedia.org/
- Plate-forme de consultation en ligne de l'ISO: disponible à l'adresse http://www.iso.org/obp
- Termes et définitions UIT: disponible à l'adresse http://www.itu.int/go/terminology-database.

**3.1** **entité**: Organisation (3.2) et autres organismes ou parties.

NOTE – Une entité peut être un groupe d'entreprises, une seule entreprise, une entreprise à but non lucratif ou toute autre entreprise. L'entité dispose du pouvoir de gouvernance de l'organisation. L'entité peut être l'organisation, par exemple dans le cas des plus petites entreprises.

**3.2** **organisation**: Partie d'une entité (3.1) qui administre et gère un système ISMS.

**3.3** **organe directeur**: Personne ou groupe de personnes ayant la responsabilité des performances et de la conformité de l'entité.

NOTE – SOURCE: norme ISO/CEI 27000:2018, 3.24, modifié – "organisme" a été remplacé par "entité".

**3.4** **haute direction**: Personne ou groupe de personnes qui dirige et contrôle une organisation (3.2) au plus haut niveau.

NOTE 1 – Source: norme ISO/CEI 9001.

NOTE 2 – La haute direction a le pouvoir de déléguer son autorité et de fournir des ressources au sein de l'organisation.

NOTE 3 – Si le champ d'application du système de gestion ne couvre qu'une partie de l'entité, alors la haute direction en réfère à l'équipe qui dirige et contrôle cette partie de l'entité. Dans cette situation, la haute direction doit rendre des comptes à l'organe directeur de l'entité.

NOTE 4 – En fonction de la taille et des ressources de l'organisation, la haute direction et l'organe directeur peuvent être identiques.

NOTE 5 – La haute direction fait rapport à l'organe directeur. [SOURCE: norme ISO/CEI 27000:2018, 3.75].

NOTE 6 – La norme ISO/CEI 37001 définit également l'organe directeur et la haute direction.

# 4 Abréviations

Aux fins de la présente Recommandation | Norme internationale, les abréviations suivantes s'appliquent:

ISMS système de gestion de la sécurité de l'information (*information security management system*)

TI technologies de l'information (*information technology*)

# 5 Utilisation et structure de la présente Recommandation | Norme internationale

La présente Recommandation | Norme internationale décrit comment fonctionne la gouvernance de la sécurité de l'information dans le cadre d'un système ISMS basé sur la norme ISO/CEI 27001, et comment les activités de gouvernance de la sécurité de l'information peuvent être liées à d'autres activités de gouvernance qui sont menées en dehors du cadre d'un système ISMS. Elle met en avant quatre processus importants ("évaluer", "diriger", "surveiller" et "communiquer") selon lesquels un système ISMS peut être structuré au sein d'une organisation, et propose des approches visant à intégrer la gouvernance de la sécurité de l'information dans les activités de gouvernance organisationnelle pour chacun de ces processus. Enfin, l'Annexe A illustre les relations entre la gouvernance organisationnelle, la gouvernance des technologies de l'information et la gouvernance de la sécurité de l'information.

Par définition, le système ISMS couvre l'ensemble de l'organisation (voir la norme ISO/CEI 27000). Il peut couvrir l'ensemble de l'entité ou une partie de l'entité, comme le montre la Figure B.1.

# 6 Normes de gouvernance et de gestion

## 6.1 Vue d'ensemble

La gouvernance de la sécurité de l'information est le moyen par lequel l'organe directeur d'une organisation assure la direction générale et le contrôle des activités qui influent sur la sécurité des informations de l'organisation. La direction et le contrôle de ces activités sont ciblés sur des situations dans lesquelles des dispositions de sécurité de l'information insuffisantes peuvent avoir des effets néfastes sur la capacité de l'organisation à atteindre ses objectifs généraux. L'organe directeur atteint souvent ses objectifs de gouvernance:

- en fixant un cap au moyen de l'établissement de stratégies et de politiques;
- en surveillant les résultats de l'organisation; et
- en évaluant les propositions et les plans élaborés par les responsables.

La gestion de la sécurité de l'information est liée à la garantie d'atteindre les objectifs de l'organisation présentés dans les stratégies et politiques établies par l'organe directeur. À cette fin, il est notamment possible d'interagir avec celui-ci:

- en lui présentant des propositions et des plans qu'il doit examiner; et
- en lui fournissant des informations relatives aux résultats de l'organisation.

Pour que la gouvernance de la sécurité de l'information soit efficace, il est nécessaire que les membres de l'organe directeur et les responsables remplissent leurs missions respectives de façon cohérente.

## 6.2 Activités de gouvernance dans le cadre d'un système ISMS

La norme ISO/CEI 27001 contient des précisions sur les exigences relatives à l'établissement, à la mise en œuvre, à la gestion et à l'amélioration continue d'un système de gestion de la sécurité de l'information dans le cadre d'une organisation. Elle comporte aussi des exigences relatives à l'évaluation et au traitement des risques en matière de sécurité de l'information adaptées aux besoins de l'organisation.

Le terme "gouvernance" n'est pas utilisé dans la norme ISO/CEI 27001, mais un certain nombre d'exigences, qui sont des activités de gouvernance, y sont décrites. La liste ci-dessous comporte des exemples de ces activités. Les références à l'organisation et à la haute direction sont liées au champ d'application d'un système ISMS basé sur la norme ISO/CEI 27001, comme indiqué précédemment.

- Aux termes du paragraphe 4.1 de la norme ISO/CEI 27001:2013, l'organisation est tenue d'identifier ce à quoi elle veut parvenir, c'est-à-dire ses buts et objectifs en matière de sécurité de l'information. Ceux-ci devraient être liés aux buts et objectifs généraux de l'entité, et les appuyer. Cela se rapporte aux objectifs de gouvernance 1, 3 et 4 décrits dans le paragraphe 7.2 de la présente Recommandation | Norme internationale.
- Aux termes du paragraphe 4.2 de la norme ISO/CEI 27001:2013, l'organisation est tenue d'identifier les parties qui sont concernées par son système ISMS, c'est-à-dire les parties intéressées, ainsi que les exigences de celles-ci en matière de sécurité de l'information. Cela se rapporte à l'objectif de gouvernance 4 décrit dans le paragraphe 7.2 de la présente Recommandation | Norme internationale.
- Aux termes du paragraphe 4.3 de la norme ISO/CEI 27001:2013, l'organisation est tenue de définir les limites et les possibilités d'application du système ISMS, afin de déterminer son domaine d'application en tenant compte des problématiques internes et externes, des exigences, des interfaces et des dépendances. Il est également indiqué que l'organisation doit intégrer les exigences et les attentes des parties intéressées dans son système de gestion de la sécurité de l'information, ainsi que les problématiques internes et externes (comme les lois, les réglementations et les contrats). Cela se rapporte à l'objectif de gouvernance 1 décrit dans le paragraphe 7.2 de la présente Recommandation | Norme internationale.
- Dans le paragraphe 5 de la norme ISO/CEI 27001:2013, il est indiqué que l'organisation doit définir une politique et des objectifs, et intégrer la sécurité de l'information dans ses processus (dont on peut envisager qu'ils incluent les processus de gouvernance). Aux termes de ce paragraphe, l'organisation est tenue de mettre des ressources adéquates à disposition et de faire comprendre l'importance de la gestion de la sécurité de l'information. Plus important encore, elle est également tenue d'orienter et de soutenir les personnes pour contribuer à l'efficacité du système ISMS, et de soutenir d'autres personnes assurant des fonctions de gestion importantes dans leurs domaines de responsabilité. Le paragraphe 5 de la norme ISO/CEI 27001:2013 contient des instructions relatives à la définition de politiques et à l'attribution de fonctions ayant trait à la gestion de la sécurité de l'information et à la présentation de rapports. Cela se rapporte aux objectifs de gouvernance 1 et 3 décrits dans le paragraphe 7.2 de la présente Recommandation | Norme internationale.
- Le paragraphe 6 de la norme ISO/CEI 27001:2013 porte sur l'élaboration d'une approche en matière de gestion des risques pour l'organisation. Il est précisé que l'organisation doit identifier les risques et les opportunités dont elle doit tenir compte pour garantir l'efficacité de son système ISMS. Ce paragraphe présente le concept de pilotes de risques, et décrit leurs missions dans le cadre des activités de l'organisation, qui consistent à gérer les risques et approuver les activités de traitement des risques. Il est également demandé à l'organisation de définir des objectifs en matière de sécurité de l'information. Cela se rapporte à l'objectif de gouvernance 2 décrit dans le paragraphe 7.2 de la présente Recommandation | Norme internationale.
- Le paragraphe 7 de la norme ISO/CEI 27001:2013 indique que les personnes doivent être aptes à remplir leurs obligations en matière de sécurité de l'information, et contient une exigence relative aux communications organisationnelles. Cela se rapporte à l'objectif de gouvernance 5 décrit dans le paragraphe 7.2 de la présente Recommandation | Norme internationale.
- Le paragraphe 8 de la norme ISO/CEI 27001:2013 dispose que l'organisation est responsable de la planification, de la mise en œuvre et du contrôle de son système ISMS, y compris des services externalisés. Cela se rapporte aux objectifs de gouvernance 4 et 6 décrits dans le paragraphe 7.2 de la présente Recommandation | Norme internationale.
- Le paragraphe 9 de la norme ISO/CEI 27001:2013 exige de contrôler tous les aspects importants du système ISMS, les audits internes, l'examen et les décisions de la haute direction et de l'organe directeur concernant l'efficacité opérationnelle du système ISMS, y compris tous les changements nécessaires, et de faire rapport sur ce qui précède. Cela se rapporte à l'objectif de gouvernance 6 décrit dans le paragraphe 7.2 de la présente Recommandation | Norme internationale.

- Le paragraphe 10 de la norme ISO/CEI 27001:2013 donne des précisions sur l'identification et le traitement des cas de non-conformité, la nécessité d'identifier des possibilités d'amélioration continue et les actions à mener sur la base de ces opportunités. Cela se rapporte à l'objectif de gouvernance 4 décrit dans le paragraphe 7.2 de la présente Recommandation | Norme internationale.

### 6.3 Autres normes connexes

La norme ISO/CEI 38500 fournit aux membres des organes directeurs des organisations des principes directeurs concernant l'utilisation efficace, efficiente et acceptable des technologies de l'information dans leurs organisations. Elle fournit aussi des indications aux personnes qui conseillent, informent ou aident les organes directeurs en matière de gouvernance des technologies de l'information.

### 6.4 Fil conducteur de la gouvernance au sein de l'organisation

Les éléments suivants, qui constituent le fil conducteur de la gouvernance, correspondent exactement aux processus de gouvernance organisationnelle décrits dans le paragraphe 7. Les deux derniers points de la liste sont les équivalents de leurs aspects de gouvernance dans le contexte de la sécurité de l'information:

- harmonisation des objectifs de sécurité de l'information avec les objectifs opérationnels;
- conformité de la gestion des risques en matière de sécurité de l'information avec les objectifs de sécurité de l'information;
- prévention des conflits d'intérêt dans la gestion de la sécurité de l'information;
- empêcher que les technologies de l'information de l'organisation soient utilisées dans le but de nuire à d'autres organisations.

## 7 Gouvernance de l'entité et gouvernance de la sécurité de l'information

### 7.1 Vue d'ensemble

Il existe de nombreux domaines de gouvernance au sein d'une entité, dont la sécurité de l'information, les technologies de l'information, la santé et la sécurité, la qualité et les finances. Chaque domaine de gouvernance est une composante des objectifs de gouvernance d'ordre général d'une entité et devrait donc concorder avec la discipline de l'entité. Parfois, les domaines d'application des modèles de gouvernance se chevauchent. Les paragraphes 7.2 et 7.3 décrivent les objectifs et processus inhérents à la gouvernance de la sécurité de l'information, qui peuvent s'appliquer à tout domaine gouverné.

Un système ISMS est axé sur la gestion des risques liés à l'information. Il ne tient pas compte directement de questions telles que la rentabilité, l'acquisition, l'utilisation et la réalisation de biens, ou l'efficacité d'autres processus, même s'il devrait appuyer tous les objectifs organisationnels qui se rapportent à ces questions.

### 7.2 Objectifs

#### 7.2.1 Objectif 1: Instaurer la sécurité de l'information intégrée et globale à l'échelle de l'entité

La gouvernance de la sécurité de l'information devrait veiller à ce que les objectifs en matière de sécurité de l'information soient globaux et intégrés. La sécurité de l'information devrait être administrée au niveau de l'entité et les décisions devraient tenir compte des priorités de l'entité. Il convient de coordonner étroitement les activités se rapportant à la sécurité physique et logique. Il n'est toutefois pas nécessaire de mettre en place un seul ensemble de mesures de sécurité ou système de gestion de la sécurité de l'information (ISMS) au sein de l'entité.

Pour garantir la sécurité de l'information à l'échelle de l'entité, l'ensemble des activités d'une entité devrait être soumis à l'obligation de responsabilité et à l'obligation de rendre des comptes en matière de sécurité de l'information. Cet aspect peut dépasser les "frontières" d'une entité telles qu'on les perçoit traditionnellement, par exemple pour inclure des informations stockées ou transférées par des parties extérieures.

#### 7.2.2 Objectif 2: Prendre des décisions en utilisant une approche fondée sur les risques

La gouvernance de la sécurité de l'information devrait reposer sur des obligations de conformité, ainsi que sur des décisions prises en fonction des risques propres à l'entité. Le niveau de sécurité acceptable devrait être déterminé selon les risques qu'une entité est prête à prendre (perte d'un avantage concurrentiel, risques sur le plan de la conformité et de la responsabilité, perturbations opérationnelles, réputation ternie et pertes financières, par exemple).

La gestion des risques en matière de sécurité de l'information devrait être uniforme dans toute l'entité et tenir compte des effets néfastes des failles et des cas de non-conformité sur les finances, les opérations et la réputation. De plus, la gestion des risques liés à la sécurité de l'information devrait être intégrée dans l'approche globale de l'entité en matière de gestion des risques, de façon à ce qu'elle ne s'effectue pas de manière isolée et qu'elle ne soit pas source de confusion. Ainsi, par exemple, cela permettrait d'établir une correspondance avec la méthode de l'entité ou de rendre compte des risques liés aux informations stratégiques dans le registre des risques de l'entité.

Pour mettre en œuvre une gestion des risques liés à la sécurité de l'information, des ressources suffisantes devraient être affectées au titre du processus de gouvernance de la sécurité.

### 7.2.3 Objectif 3: Définir des orientations pour les acquisitions

Il convient d'évaluer de manière adéquate les effets des risques en matière de sécurité de l'information au moment d'entreprendre de nouvelles activités, notamment, sans toutefois s'y limiter, tout investissement, achat, fusion, adoption de nouvelles technologies, accord d'externalisation et contrat avec des fournisseurs externes.

Pour optimiser les acquisitions en matière de sécurité de l'information destinées à appuyer la réalisation des objectifs de l'entité, l'organe directeur devrait veiller à ce que la sécurité de l'information soit intégrée aux processus en vigueur dans l'entité, notamment ceux qui concernent la gestion de projets, les achats, les dépenses financières, la conformité aux cadres juridiques et réglementaires et la gestion des risques d'ordre stratégique.

La haute direction du système ISMS devrait mettre en place une stratégie en matière de sécurité de l'information fondée sur les objectifs de l'entité, de façon à garantir l'harmonisation entre les besoins de l'entité et les exigences de sécurité de l'information d'ordre organisationnel, et à répondre ainsi aux besoins actuels et changeants des parties intéressées.

### 7.2.4 Objectif 4: Veiller au respect des obligations internes et externes

Dans le cadre de la gouvernance de la sécurité de l'information, les politiques et pratiques en matière de sécurité de l'information devraient être conformes aux obligations des parties intéressées. Il peut s'agir d'obligations législatives et réglementaires, d'obligations contractuelles et d'engagements internes.

Pour résoudre les problèmes liés à la conformité et au respect des dispositions, la haute direction peut obtenir l'assurance que les activités liées à la sécurité de l'information satisfont aux obligations internes et externes en demandant des audits de sécurité indépendants.

### 7.2.5 Objectif 5: Favoriser une culture propice à la sécurité

La gouvernance de la sécurité de l'information devrait reposer sur la culture de l'entité, y compris les besoins en évolution de toutes les parties intéressées, dans la mesure où le comportement humain est l'un des éléments essentiels pour assurer le niveau approprié de sécurité de l'information. Faute d'une coordination adéquate, il risque d'y avoir contradiction entre les objectifs, les rôles, les responsabilités et les ressources, ce qui nuira à la réalisation de tout objectif. Par conséquent, il est très important d'assurer une harmonisation et de définir des orientations concertées entre toutes les parties intéressées.

Pour créer une véritable culture de la sécurité de l'information, la haute direction devrait exiger, favoriser et appuyer la coordination des activités des parties intéressées pour définir une orientation cohérente en matière de sécurité de l'information, ce qui facilitera la mise en œuvre de programmes d'enseignement, de formation et de sensibilisation dans le domaine de la sécurité. Les responsabilités en matière de sécurité de l'information devraient être intégrées dans le rôle des membres du personnel et des autres parties et ces derniers devraient contribuer à la réussite de chaque système ISMS en assumant ces responsabilités.

### 7.2.6 Objectif 6: Garantir que l'efficacité de la sécurité réponde aux besoins actuels et futurs de l'entité

Dans le cadre de la gouvernance de la sécurité de l'information, il convient de veiller à ce que l'approche retenue pour protéger l'information soit adaptée aux besoins de l'entité, en assurant les niveaux convenus de sécurité de l'information. Il faudrait surveiller et maintenir l'efficacité de la sécurité aux niveaux requis pour répondre aux besoins actuels et futurs.

Pour évaluer l'efficacité de la sécurité de l'information du point de vue de la gouvernance, l'organe directeur devrait évaluer cette efficacité sous l'angle de ses incidences sur l'entité, et pas uniquement du point de vue de l'efficacité et de l'efficience des contrôles de sécurité.

La haute direction de chaque système ISMS devrait être chargée de mettre en œuvre, au sein de ce système, un programme d'évaluation de l'efficacité à des fins de suivi, d'audit et d'identification de possibilités d'amélioration. L'organe directeur devrait rattacher l'efficacité de la sécurité de l'information et les résultats obtenus par l'organisation et l'entité.

## 7.3 Processus

### 7.3.1 Généralités

L'organe directeur au sein d'une entité mène à bien les processus "évaluer", "diriger", "surveiller" et "communiquer". La Figure 1 montre les liens entre ces processus.

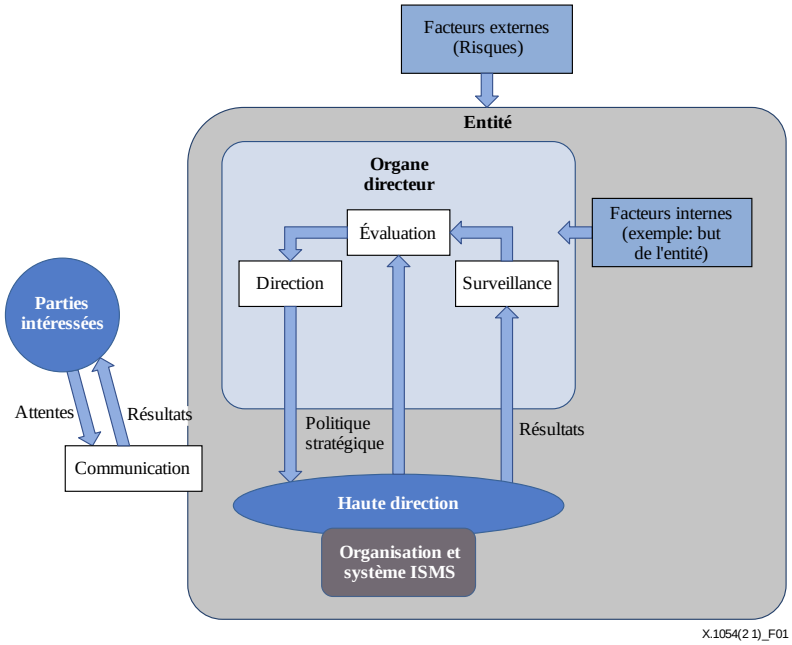


**Figure 1 – Modèle de gouvernance pour une entité disposant d'un système ISMS**

NOTE 1 – Selon la définition d'"organisation" [3.2], la haute direction est toujours pleinement impliquée dans le fonctionnement de l'organisation.

NOTE 2 – Une entité peut contenir plus d'un système ISMS et il est possible que certaines parties d'une entité concernée par la gouvernance ne fassent pas partie d'un système ISMS. Voir le paragraphe 8 et l'Annexe B.

### 7.3.2 Évaluer

"L'évaluation" est le processus de gouvernance qui consiste à examiner le niveau effectif et prévu de réalisation des objectifs à partir des processus actuels et des changements prévus, puis à déterminer les éventuels ajustements nécessaires pour optimiser la réalisation des objectifs stratégiques dans l'avenir.

Pour mener à bien le processus d'"évaluation":

– l'organe directeur de l'entité devrait:
  - faire en sorte que les initiatives prises tiennent compte des risques et des opportunités pertinents;
  - tirer les enseignements des mesures et des rapports concernant la sécurité de l'information et le système ISMS en fixant les objectifs à atteindre dans le cadre de chaque système ISMS et en hiérarchisant ces objectifs (cela inclut l'examen des exigences qui n'entrent pas dans le cadre du système ISMS); et
– la haute direction de chaque système ISMS devrait:
  - faire en sorte que la sécurité de l'information favorise et soutienne la réalisation des objectifs de l'entité;
  - soumettre à l'organe directeur, pour approbation, de nouveaux projets sur la sécurité de l'information ayant une grande incidence.

### 7.3.3 Diriger

La "direction" est le processus de gouvernance dans le cadre duquel l'organe directeur donne des orientations sur les objectifs et la stratégie de l'entité. Il peut s'agir de modifier le niveau et l'affectation des ressources ou l'ordre de priorité des activités, ou d'approuver des politiques ainsi que des plans d'acceptation des risques matériels et de gestion des risques.

Pour mener à bien le processus de "direction":

– l'organe directeur devrait:

- fixer les orientations stratégiques générales et les objectifs de l'entité;
- définir le niveau de risque accepté par l'entité;
- approuver la stratégie en matière de sécurité de l'information; et

– la haute direction de chaque système ISMS devrait:

- engager les investissements et les ressources nécessaires;
- faire concorder les objectifs de sécurité de l'information d'ordre organisationnel avec les objectifs de l'entité;
- attribuer des rôles et des responsabilités en matière de sécurité de l'information;
- établir une politique de sécurité de l'information.

NOTE – La propension au risque est le degré et le type de risque qu'une organisation est disposée à prendre ou à conserver. [8]

### 7.3.4 Surveiller

La "surveillance" est le processus de gouvernance qui permet à l'organe directeur d'évaluer dans quelle mesure les objectifs stratégiques sont atteints.

Pour mener à bien le processus de "surveillance":

– l'organe directeur devrait:

- recevoir un rapport sur l'efficacité du fonctionnement de chaque système ISMS;
- évaluer l'efficacité du fonctionnement du système ISMS au regard des priorités de l'entité;
- présenter les priorités à la haute direction de chaque système ISMS; et

– la haute direction de chaque système ISMS devrait:

- évaluer l'efficacité des activités de gestion de la sécurité de l'information;
- veiller au respect des obligations internes et externes;
- examiner l'évolution de l'entité, du contexte juridique et réglementaire, et toute incidence possible sur les risques liés à l'information;
- choisir des critères de performance appropriés et demander que les rapports soient présentés dans un délai convenable du point de vue de l'organisation;
- communiquer à l'organe directeur les résultats obtenus en matière de sécurité de l'information;
- alerter l'organe directeur sur les faits nouveaux ayant une incidence sur les risques liés à l'information et sur la sécurité de l'information.

Pour évaluer l'efficacité de la sécurité de l'information du point de vue de la gouvernance, la haute direction devrait évaluer cette efficacité sous l'angle de ses incidences sur l'organisation et l'entité, et pas uniquement du point de vue de l'efficacité et de l'efficience des contrôles de sécurité. Pour ce faire, il est possible de mettre en œuvre un programme d'évaluation de l'efficacité à des fins de suivi, d'audit et d'identification de possibilités d'amélioration, de façon à rattacher l'efficacité de la sécurité de l'information et les résultats obtenus par l'organisation et l'entité.

### 7.3.5 Communiquer

La "communication" est le processus de gouvernance bidirectionnel par lequel l'organe directeur et les parties intéressées échangent des informations en fonction de leurs besoins particuliers.

Une méthode de "communication" possible consiste à établir un compte rendu sur l'état de la sécurité de l'information qui présente aux parties intéressées des renseignements sur les activités menées dans ce domaine et les problèmes rencontrés.

Le processus de communication permet notamment de tenir les entités pour responsables devant les parties intéressées, comme les actionnaires. Cet aspect gagne en importance, et les organisations fournissent maintenant des renseignements sur la mise en œuvre et la maintenance de leur système de gestion de la sécurité de l'information, ainsi que sur son efficacité en matière de gestion des risques. Aussi, après qu'un incident lié à la sécurité de l'information se soit produit, les entités devraient expliquer aux parties intéressées, et séparément au grand public le cas échéant, les effets et la cause de l'incident, ainsi que les changements apportés aux contrôles pour que l'incident ne se reproduise plus.

Des méthodes diverses peuvent être utilisées dans le processus de communication. Le contenu d'une communication est également varié, et elle sera également adressée à des publics différents. Toute communication devrait être élaborée en tenant compte du public visé et du message que l'on souhaite lui faire passer. Ces deux facteurs devraient alors être pris en considération pour décider du contenu des communications et des canaux à utiliser pour les adresser au public visé. Un exemple est présenté dans l'Annexe C.

Pour mener à bien le processus de "communication":

– l'organe directeur devrait:
  - informer les parties intéressées externes que l'entité applique un niveau de sécurité de l'information adapté à la nature de ses activités et priorités;
  - identifier et hiérarchiser les obligations réglementaires, les attentes des parties intéressées et les besoins de l'entité en matière de sécurité de l'information;
  - informer la haute direction de chaque système ISMS de tout problème qui doit retenir son attention et appelle une décision;
  - donner aux parties intéressées concernées des instructions concernant les objectifs détaillés à réaliser à l'appui des priorités en matière de sécurité de l'information;
  - promouvoir une véritable culture de la sécurité de l'information;
  - former les membres du personnel et d'autres personnes à leurs responsabilités dans le cadre du système ISMS, et communiquer avec eux à ce sujet.

# 8 Besoins de l'organe directeur concernant le système ISMS

## 8.1 Organisation et système ISMS

L'organe directeur devrait demander qu'un ou plusieurs systèmes ISMS soient conçus afin d'appuyer les objectifs de l'entité. Les objectifs de chaque système ISMS peuvent être identiques ou non à ceux de l'entité parente selon la taille, l'envergure et la structure de l'entité entière, mais ils devraient concorder. Les relations possibles entre la gouvernance de la sécurité de l'information et la gouvernance des technologies de l'information sont illustrées dans l'Annexe A.

En outre, l'organe directeur devrait demander que chaque système ISMS soit conçu de sorte qu'il cadre bien avec les politiques et processus d'ordre général de l'entité, y compris la gestion des risques. Il peut être opportun qu'un système ISMS adopte le même processus d'évaluation des risques que l'organe directeur, afin que la communication des informations sur les risques soit claire. Si l'organe directeur utilise un processus d'évaluation des risques non conforme aux prescriptions établies dans la norme ISO/CEI 27001, alors, si l'organisation souhaite se conformer à ces prescriptions, son système ISMS devrait utiliser une approche en matière d'évaluation des risques différente de celle utilisée par l'entité, et convenir d'une méthode de communication des informations relatives aux risques à l'organe directeur dans des termes compatibles avec l'approche de l'organe directeur. Sinon, l'organe directeur peut choisir de modifier le processus d'évaluation des risques en vigueur de l'entité pour respecter les prescriptions établies dans la norme ISO/CEI 27001.

L'organe directeur peut exiger qu'un système ISMS soit utilisé pour gérer les risques stratégiques liés à la perte de droits de propriété intellectuelle, à l'atteinte à la réputation et à des pertes financières associées à des atteintes à la confidentialité, à l'intégrité ou à la disponibilité des informations.

Un système ISMS peut fournir à l'organe directeur des informations de gestion concernant:

- les risques pour l'entité;
- l'efficacité du système ISMS.

L'organe directeur devrait:

- approuver la création de chaque système ISMS;
- définir le champ d'application de chaque système ISMS et de la certification (ces champs d'application peuvent différer);
- donner des orientations à chaque système ISMS, y compris définir des objectifs et des exigences, attribuer des rôles et affecter des ressources;
- prendre des décisions concernant les niveaux acceptables de risques résiduels ou les traitements des risques appropriés;
- fournir à chaque système ISMS des canaux de communication et lui donner l'autorisation de les utiliser pour communiquer les informations utiles aux parties intéressées et à toutes les personnes qui interviennent dans le champ de ce système ISMS.

## 8.2 Scénarios (voir l'Annexe B)

### 8.2.1 Type A: L'organisation ISMS est l'entité entière

Si le seul système de gestion en place est conforme à la norme ISO/CEI 27001, il peut être utilisé pour fournir des informations sur les risques, ce qui permet ainsi à une organisation de gérer les risques liés à l'information. Cependant, il existe toujours différents processus pour appuyer la gouvernance des technologies de l'information, des finances, des opérations et d'autres activités de gouvernance.

Dans le cas où l'organisation ISMS désigne l'entité entière:

- Les processus de gouvernance décrits dans le paragraphe 7.3 sont inchangés.
- La haute direction assume des responsabilités de gouvernance outre celle de gouvernance de la sécurité de l'information, comme la gouvernance institutionnelle.

Il est probable que l'harmonisation entre les objectifs de sécurité de l'information de l'organisation et les objectifs généraux de l'entité se fasse sans aucun problème, puisque la haute direction est chargée de définir aussi bien les premiers que les seconds. S'il existe un seul rôle de responsable à la fois de la gouvernance et de la gestion de la sécurité de l'information, il convient de dispenser des conseils adéquats pour garantir que la responsabilité de définir les politiques et celle de les exécuter soient bien séparées l'une de l'autre.

### 8.2.2 Type B: L'organisation ISMS fait partie d'une entité plus large

Certaines organisations ISMS font partie d'une entité plus large. Étant donné que les activités de gouvernance s'appliquent habituellement à l'ensemble d'une entité juridique, d'une société, d'une association caritative, d'un organisme public ou de toute autre entité, la gouvernance de cette entité déborde dans ce cas du cadre du système ISMS. Une organisation peut avoir plusieurs systèmes ISMS en son sein. Par conséquent, un organe directeur peut administrer de multiples systèmes ISMS. La majeure partie du présent document vise à permettre cette approche.

Les quatre processus de gouvernance décrits dans le paragraphe 7.3 restent pertinents. Toutefois, en fonction de la relation entre l'organisation/les organisations ISMS et l'entité parente, l'une des situations suivantes peut s'appliquer:

- Chaque organisation ISMS fonctionne comme une partie autonome de l'entité parente et a donc ses propres objectifs opérationnels. Dans ce cas, les objectifs de sécurité de l'information de l'organisation ISMS devraient concorder avec ses propres objectifs opérationnels.
- Chaque organisation ISMS est chargée d'atteindre au moins un des objectifs opérationnels de l'entité parente. Dans ce cas, les objectifs de sécurité de l'information de l'organisation ISMS devraient concorder avec les objectifs opérationnels de son entité parente.

Chaque organisation ISMS s'est vu attribuer la responsabilité de gérer un aspect des risques en matière de sécurité de l'information au nom de l'entité parente. Dans ce cas, les objectifs de sécurité de l'information de l'organisation ISMS devraient être définis par l'entité parente, ce qui garantira leur concordance avec les objectifs opérationnels de l'entité parente.

Il existe aussi une relation entre la haute direction de chaque organisation ISMS et l'organe directeur de l'entité parente. L'équipe/les équipes de haute direction et l'organe directeur peuvent être identiques, avoir plusieurs membres en commun, ou n'avoir aucun membre en commun. La Figure B.1 devrait être utilisée pour désigner les personnes qui devraient figurer parmi les membres de l'organe directeur ou les parties intéressées.

### 8.2.3 Type C: L'organisation ISMS est composée de parties de plusieurs entités

Dans cette situation, l'organisation ISMS est administrée et contrôlée par la haute direction, comme d'habitude, mais elle recouvre plusieurs entités. Cela peut arriver si une entité plus large dirige un groupe d'entités qui partagent un contexte commun concernant la sécurité de l'information et des exigences communes applicables à un sous-ensemble de leurs activités, par exemple lorsque des données personnelles sont recueillies, traitées, stockées et utilisées pour offrir des services. Plusieurs organes directeurs peuvent aussi partager un système ISMS; par exemple, une organisation peut fournir un système ISMS en tant que service destiné à être utilisé par de nombreux consommateurs.

Dans le cas où une organisation ISMS inclut des parties de plusieurs entités:

- les processus de gouvernance décrits dans le paragraphe 7.3 sont inchangés;
- les objectifs de sécurité de l'information de l'organisation ISMS devraient concorder avec les objectifs opérationnels communs qui unissent les entités membres.

# Annexe A

## Relation de gouvernance

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale.)

La Figure A.1 illustre la relation entre la gouvernance de la sécurité de l'information et la gouvernance des technologies de l'information.

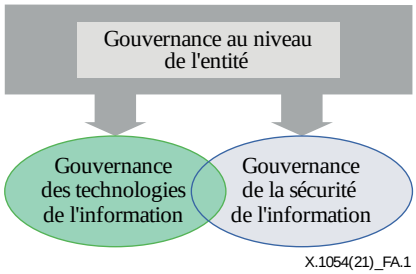


**Figure A.1 – Relation entre la gouvernance de la sécurité de l'information et la gouvernance des technologies de l'information**

La gouvernance des technologies de l'information concerne avant tout les ressources nécessaires pour obtenir, traiter, stocker et diffuser des informations, tandis que la gouvernance de la sécurité de l'information porte sur la confidentialité, l'intégrité et la disponibilité de l'information. Ces deux systèmes de gouvernance peuvent être gérés selon les processus de gouvernance suivants: évaluer, diriger, surveiller et communiquer.

# Annexe B

## Types d'organisation ISMS

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale.)

Il existe trois types de relation entre une organisation qui gère un système ISMS et une entité qui applique un système ISMS. Ces relations concernent aussi les membres de la haute direction du système ISMS et l'organe directeur de l'entité. La liste ci-dessous et la Figure B.1 illustrent ces types de relation.

Type A: L'entité et l'organisation ISMS sont identiques.

- L'organe directeur et la haute direction du système ISMS sont identiques.

Type B: L'entité inclut l'organisation ISMS (et plusieurs systèmes ISMS peuvent être en service au sein de l'entité).

- Certains membres de l'organe directeur peuvent faire partie de la haute direction d'un système ISMS, mais la composition de l'organe directeur n'est pas identique à celle de la haute direction d'un système ISMS.

Type C: Un système ISMS est partagé par plusieurs entités:

- si les entités sont directement concernées par le système ISMS, des membres de l'organe directeur de chaque entité peuvent faire partie de la haute direction du système ISMS;
- si le système ISMS est un service fourni par une tierce partie, il est peu probable que la haute direction du système ISMS soit composée de membres des organes directeurs des entités partageant le système ISMS.

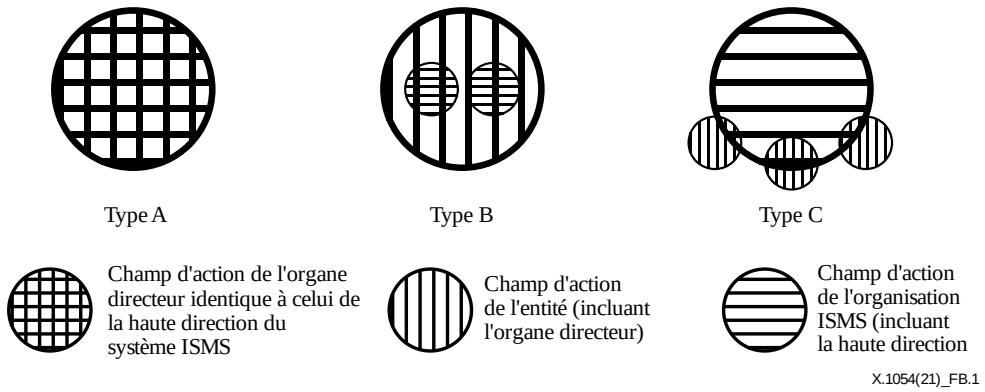


**Figure B.1 – Relations possibles entre une/des entité(s) et son/leurs système(s) ISMS**

# Annexe C

## Exemples de communication

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale.)

On peut observer un exemple de communication sur les marchés boursiers, où les entreprises sont obligées d'exposer les risques en matière de sécurité de l'information en vertu de lois ou de règles sectorielles. Le rapport sur les questions environnementales, sociales et de gouvernance (ESG) constitue un autre exemple: en effet, il permet aux organisations d'expliquer/de présenter aux parties intéressées leurs efforts en matière environnementale et socio-économique. Certains rapports ESG décrivent l'approche concernant la protection des données personnelles, les activités de sécurité de l'information et la gestion de crise en vue de prévenir les incidents touchant à la sécurité.

Lors de l'élaboration d'une communication, il convient également de tenir compte des effets imprévus qui se produisent lorsque le public ne comprend pas le contenu ou l'interprète mal, ou lorsque la communication touche des personnes ne faisant pas partie du public visé.

## Bibliographie


[1] Recommandation UIT-T X.1051 (2016) | norme ISO/CEI 27011:2016, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique basé sur la norme ISO/CEI 27002 pour la gestion de la sécurité des informations pour les organisations de télécommunication*.

[2] ISF, Standard of Good Practice for Information Security: 2018.

[3] ISO 37001:2016, *Systèmes de management anti-corruption – Exigences et recommandations de mise en œuvre.*

[4] ISO/CEI 9001:2015, *Systèmes de managements de la qualité – Exigences*.

[5] ISO/CEI 27000:2018, *Sécurité de l'information, cybersécurité et protection de la vie privée – Vue d'ensemble et vocabulaire*.

[6] ISO/CEI 27002:2013, *Sécurité de l'information, cybersécurité et protection de la vie privée – Code de bonne pratique pour le management de la sécurité de l'information*.

[7] ISO/CEI 38500:2015, *Technologies de l'information – Gouvernance des technologies de l'information pour l'entreprise*.

[8] ISO Guide 73:2009.

[9] Institut de gouvernance des technologies de l'information (IT Governance Institute – ITGI), *Information Security Governance: Guidance for Information Security Managers: 2008*.

[10] ITGI, *Information Security Governance Guidance for Boards of Directors and Executive Management*, 2nd Edition: 2006.

[11] ITGI, *COBIT Control Practices: Guidance to Achieve Control Objective for Successful IT Governance*, 2nd Edition: 2007.

[12] Ohki E., Harada Y., Kawaguchi S., Shiozaki T., Kgaua T., *Information Security Governance framework, Proceedings of the first ACM workshop on Information security governance*, pp. 1-6, 2009.

## SÉRIES DES RECOMMANDATIONS UIT-T

| | |
|---|---|
| Série A | Organisation du travail de l'UIT-T |
| Série D | Principes généraux de tarification |
| Série E | Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains |
| Série F | Services de télécommunication non téléphoniques |
| Série G | Systèmes et supports de transmission, systèmes et réseaux numériques |
| Série H | Systèmes audiovisuels et multimédias |
| Série I | Réseau numérique à intégration de services |
| Série J | Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias |
| Série K | Protection contre les perturbations |
| Série L | Construction, installation et protection des câbles et autres éléments des installations extérieures |
| Série M | Gestion des télécommunications y compris le RGT et maintenance des réseaux |
| Série N | Maintenance: circuits internationaux de transmission radiophonique et télévisuelle |
| Série O | Spécifications des appareils de mesure |
| Série P | Terminaux et méthodes d'évaluation subjectives et objectives |
| Série Q | Commutation et signalisation |
| Série R | Transmission télégraphique |
| Série S | Équipements terminaux de télégraphie |
| Série T | Terminaux des services télématiques |
| Série U | Commutation télégraphique |
| Série V | Communications de données sur le réseau téléphonique |
| **Série X** | **Réseaux de données, communication entre systèmes ouverts et sécurité** |
| Série Y | Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération |
| Série Z | Langages et aspects généraux logiciels des systèmes de télécommunication |

Imprimé en Suisse
Genève, 2022