NORME INTERNATIONALE

ISO/IEC 27011

Deuxième édition
2016-12-01

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour les contrôles de la sécurité de l'information fondés sur l'ISO/IEC 27002 pour les organismes de télécommunications

Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

Numéro de référence
ISO/IEC 27011:2016(F)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 organismes internationaux, gouvernementaux et non gouvernementaux, en liaison avec l'ISO et l'IEC participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

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.

Cette deuxième édition annule et remplace la première édition de l'ISO/IEC 27011:2008, qui a fait l'objet d'une révision technique.

L'ISO/IEC 27011 a été élaborée par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*. Le texte identique est publié en tant que Rec. ITU-T X.1051.

Sommaire

Page

1 Domaine d'application 1
2 Références normatives 1
3 Définitions et abréviations 1
3.1 Définitions 1
3.2 Abréviations 2
4 Vue d'ensemble 3
4.1 Structure de la présente Recommandation | Norme internationale 3
4.2 Systèmes de management de la sécurité de l'information dans les organismes de télécommunications 3
5 Politiques de sécurité de l'information 6
6 Organisation de la sécurité de l'information 6
6.1 Organisation interne 6
6.2 Appareils mobiles et télétravail 7
7 Sécurité des ressources humaines 8
7.1 Avant l'embauche 8
7.2 Pendant la durée du contrat 9
7.3 Rupture, terme ou modification du contrat de travail 9
8 Gestion des actifs 9
8.1 Responsabilités relatives aux actifs 9
8.2 Classification de l'information 9
8.3 Manipulation des supports 10
9 Contrôle d'accès 10
9.1 Exigence métier en matière de contrôle d'accès 10
9.2 Gestion de l'accès utilisateur 11
9.3 Responsabilités des utilisateurs 11
9.4 Contrôle de l'accès au système et aux applications 11
10 Cryptographie 11
11 Sécurité physique et environnementale 11
11.1 Zones sécurisées 11
11.2 Matériels 12
12 Sécurité liée à l'exploitation 14
12.1 Procédures et responsabilités liées à l'exploitation 14
12.2 Protection contre les logiciels malveillants 15
12.3 Sauvegarde 15
12.4 Journalisation et surveillance 15
12.5 Maîtrise des logiciels en exploitation 16
12.6 Gestion des vulnérabilités techniques 16
12.7 Considérations sur l'audit des systèmes d'information 17
13 Sécurité des communications 17
13.1 Management de la sécurité des réseaux 17
13.2 Transfert de l'information 18
14 Acquisition, développement et maintenance des systèmes 18
14.1 Exigences de sécurité applicables aux systèmes d'information 18

14.2 Sécurité des processus de développement et d'assistance technique 19
14.3 Données de test 19
15 Relations avec les fournisseurs 19
15.1 Sécurité de l'information dans les relations avec les fournisseurs 19
15.2 Gestion de la prestation de services des fournisseurs 20
16 Gestion des incidents liés à la sécurité de l'information 20
16.1 Gestion des incidents liés à la sécurité de l'information et améliorations 20
17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité 23
17.1 Continuité de la sécurité de l'information 23
17.2 Redondances 23
18 Conformité 24
Annexe A Ensemble de contrôles étendus des télécommunications 25
Annexe B Recommandations supplémentaires relatives à la sécurité des réseaux 35
B.1Mesures de sécurité contre les attaques de réseaux 35
B.2Mesures de sécurité du réseau pour la congestion des réseaux 36
Bibliographie 37

Introduction

La présente Recommandation | Norme internationale fournit des lignes directrices d'interprétation pour la mise en œuvre et la gestion des contrôles de la sécurité de l'information basés sur l'ISO/IEC 27002 dans les organismes de télécommunications.

Les organismes de télécommunications fournissent des services de télécommunications en facilitant les communications entre les clients par l'intermédiaire de leur infrastructure. Afin de fournir des services de télécommunications, les organismes de télécommunications ont besoin d'établir une interconnexion et/ou de partager leurs services et installations et/ou d'utiliser les services et installations d'autres organismes de télécommunications. De plus, l'emplacement du site, notamment les stations radio, les emplacements d'antennes, les câbles de terre et les réseaux de fourniture de services d'infrastructure (électricité, eau), peut être accessible non seulement au personnel de l'organisme, mais également à des sous-traitants et prestataires extérieurs à l'organisme.

La gestion de la sécurité de l'information dans les organismes de télécommunications peut donc être complexe et éventuellement impliquer :

- une dépendance à des parties externes ;
- la nécessité de couvrir toutes les zones de l'infrastructure réseau, des applications de services et autres installations ;
- l'inclusion d'une diversité de technologies de télécommunications (par exemple, filaires, sans fil, haut débit) ;
- la prise en charge d'une grande diversité d'échelles opérationnelles, de domaines de services et de types de services.

Outre l'application des objectifs et des mesures de sécurité décrits dans l'ISO/IEC 27002, les organismes de télécommunications peuvent avoir besoin de mettre en œuvre des mesures supplémentaires pour garantir la confidentialité, l'intégrité, la disponibilité et toute autre propriété de sécurité des télécommunications afin de gérer le risque de sécurité de façon adéquate.

1) *Confidentialité*

Protection de la confidentialité des informations relatives aux télécommunications contre une divulgation non autorisée. Cela implique la non-divulgation de communications eu égard à l'existence, au contenu, à la source, à la destination et aux date et heure des informations communiquées.

Il est essentiel que les organismes de télécommunications empêchent toute violation du principe de non-divulgation des communications qu'ils gèrent. Cela consiste notamment à s'assurer que les personnes engagées par l'organisme de télécommunications préservent la confidentialité de toute information concernant des tiers dont ils peuvent avoir eu connaissance dans l'exercice de leurs fonctions.

NOTE Le terme « secret des communications » est utilisé dans certains pays dans le contexte de la « non-divulgation de communications ».

2) *Intégrité*

La protection de l'intégrité des informations de télécommunications consiste à contrôler l'installation et l'utilisation des installations de télécommunications afin de garantir l'authenticité, l'exactitude et l'exhaustivité des informations transmises, relayées ou reçues par liaison filaire, radio ou autre.

3) *Disponibilité*

La disponibilité des informations de télécommunications consiste à s'assurer que l'accès aux installations et au support utilisés pour la fourniture des services de communication est autorisé, que ces communications soient fournies par liaison filaire, radio ou autre. En règle générale, les organismes de télécommunications donnent priorité aux communications essentielles en cas d'urgence, en gérant l'indisponibilité des communications de moindre importance conformément aux exigences réglementaires.

Public visé

La présente Recommandation | Norme internationale s'adresse aux organismes de télécommunications et aux personnes responsables de la sécurité de l'information ; ainsi qu'aux fournisseurs de solutions de sécurité, auditeurs, fournisseurs de terminaux de télécommunications et fournisseurs de contenus applicatifs. La présente Recommandation | Norme internationale fournit un ensemble commun d'objectifs généraux de contrôle de la sécurité fondés sur l'ISO/IEC 27002, des mesures spécifiques au secteur des télécommunications et des lignes directrices pour la gestion de la sécurité de l'information permettant le choix et la mise en œuvre de telles mesures.

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour les contrôles de la sécurité de l'information fondés sur l'ISO/IEC 27002 pour les organismes de télécommunications

1 Domaine d'application

Le domaine d'application de la présente Recommandation | Norme internationale est de fournir des lignes directrices qui étayent la mise en œuvre de contrôles de la sécurité de l'information dans les organismes de télécommunications.

L'adoption de la présente Recommandation | Norme internationale permettra aux organismes de télécommunications de satisfaire aux exigences de référence en matière de gestion de la sécurité de l'information concernant la confidentialité, l'intégrité, la disponibilité et toute autre propriété de sécurité pertinente.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations | Normes internationales sont sujettes à révision et les parties prenantes des 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 l'IEC et de l'ISO possèdent le registre des Normes Internationales en vigueur à un moment donné. Le Bureau de la Normalisation des Télécommunications de l'UIT tient à jour une liste de Recommandations de l'UIT-T actuellement valides.

- ISO/IEC 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*
- ISO/IEC 27002:2013, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

3 Définitions et abréviations

3.1 Définitions

Pour les besoins de la présente Recommandation | Norme internationale, les définitions données dans l'ISO/IEC 27000 et les suivantes s'appliquent.

3.1.1 co-localisation : montage d'installations de télécommunications dans les locaux d'autres opérateurs de télécommunications

3.1.2 centre de communication : bâtiment où sont situées des installations pour la fourniture d'activités de télécommunications

3.1.3 communications essentielles : communications dont le contenu est nécessaire pour la prévention de catastrophes ou l'aide déployée en cas de catastrophes, et pour le maintien de l'ordre public dans des conditions défavorables

3.1.4 non-divulgation de communications : exigence consistant à ne pas divulguer l'existence, le contenu, la source, la destination et les date et heure des informations communiquées

3.1.5 appel prioritaire : télécommunications établies par des terminaux spécifiques en cas d'urgence, qu'il convient de traiter en priorité par une limitation des appels publics

NOTE Les terminaux spécifiques peuvent couvrir différents services (voix sur IP (VoIP), réseau téléphonique public commuté, trafic de données IP, etc.) pour les réseaux filaires et sans fil.

3.1.6 applications de télécommunications : applications telles que voix sur IP (VoIP, Voice over IP), consommées par l'utilisateur final et basées sur les services en réseau

3.1.7 activité de télécommunications : activité consistant à fournir des services de télécommunications afin de répondre à la demande d'autres personnes

3.1.8 salle d'équipement de télécommunications : site ou local sécurisé dans un bâtiment général où est situé l'équipement de fourniture d'activités de télécommunications

3.1.9 installations de télécommunications : machines, équipements, fils et câbles, bâtiments physiques ou autres installations électriques pour le fonctionnement des télécommunications

3.1.10 organismes de télécommunications : entités commerciales qui fournissent des services de télécommunications afin de répondre à la demande d'autres personnes

3.1.11 registres de télécommunications : informations concernant les parties à une communication, excluant le contenu de la communication, l'heure et la durée de la télécommunication

3.1.12 services de télécommunications : communications utilisant des installations de télécommunications ou d'autres moyens de fournir des communications soit entre des utilisateurs de services de télécommunications, soit entre des clients de services de télécommunications

3.1.13 client de services de télécommunications : personne ou organisme qui signe un contrat avec des organismes de télécommunications afin que lui soient fournis des services de télécommunications

3.1.14 utilisateur de services de télécommunications : personne ou organisme qui utilise des services de télécommunications

3.1.15 installations de terminal : installations de télécommunications qui sont connectées à une extrémité des installations du circuit de télécommunications et dont une partie est destinée à être installée dans les mêmes locaux (y compris les zones considérées comme étant les mêmes locaux) ou dans le même bâtiment où il est prévu d'installer également une autre partie de ces installations

3.1.16 utilisateur : personne ou organisme qui utilise des installations ou systèmes de traitement de l'information, par exemple employé, sous-traitant ou utilisateur tiers

3.2 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes s'appliquent.

CID	Confidentialité, Intégrité et Disponibilité
CNI	Infrastructure nationale critique (*Critical National Infrastructure*)
DDoS	Déni de service distribué (*Distributed Denial of Service*)
DNS	Système de nom de domaine (*Domain Name System*)
DoS	Déni de service (*Denial of Service*)
HVAC	Chauffage, ventilation et climatisation (*Heating, Ventilation and Air Conditioning*)
IP	Protocole Internet (*Internet Protocol*)
IRC	Discussion relayée par Internet (*Internet Relay Chat*)
ISAC	Centre de partage et d'analyse d'informations (*Information Sharing and Analysis Centre*)
NMS	Système de gestion de réseau (*Network Management System*)
OAM&P	Opérations, Administration, Maintenance et Provisionnement
RTPC	Réseau Téléphonique Public Commuté

SIP	Protocole d'initiation de session (*Session Initiation Protocol*)
SLA	Accord de niveau de service (*Service Level Agreement*)
SMS	Service de messagerie courte (*Short Message Service*)
SMSI	Système de management de la sécurité de l'information
SOA	Déclaration d'applicabilité (*Statement of Applicability*)
URL	Localisateur de ressources universel (*Uniform Resource Locator*)
VoIP	Voix sur protocole Internet (*Voice over Internet Protocol*)

4 Vue d'ensemble

4.1 Structure de la présente Recommandation | Norme internationale

La présente Recommandation | Norme internationale a été structurée dans un format similaire à celui de l'ISO/IEC 27002. Dans les cas où les objectifs et mesures spécifiés dans l'ISO/IEC 27002 sont applicables sans nécessiter d'informations supplémentaires, seule la référence à l'ISO/IEC 27002 est fournie. Un ensemble de recommandations de mesure et de mise en œuvre spécifiques au secteur des télécommunications est décrit dans l'Annexe A normative.

Dans les cas où des mesures nécessitent des recommandations supplémentaires propres aux télécommunications, la mesure de l'ISO/IEC 27002 est répétée sans modification, suivie des recommandations spécifiques aux télécommunications en lien avec cette mesure. Des recommandations et des informations spécifiques au secteur des télécommunications sont fournies dans les articles suivants :

- Organisation de la sécurité de l'information (Article 6) ;
- Sécurité des ressources humaines (Article 7) ;
- Gestion des actifs (Article 8) ;
- Contrôle d'accès (Article 9) ;
- Sécurité physique et environnementale (Article 11) ;
- Sécurité liée à l'exploitation (Article 12) ;
- Sécurité des communications (Article 13) ;
- Acquisition, développement et maintenance des systèmes d'information (Article 14) ;
- Relations avec les fournisseurs (Article 15) ;
- Gestion des incidents liés à la sécurité de l'information (Article 16) ;
- Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité (Article 17).

4.2 Systèmes de management de la sécurité de l'information dans les organismes de télécommunications

4.2.1 Objectif

L'information est un élément critique pour chaque organisme. Dans le cas des télécommunications, les informations se composent des données transmises entre deux points dans une formation électronique, ainsi que des métadonnées de chaque transmission, par exemple les données de positionnement de l'expéditeur et du récepteur. Quelle que soit la manière dont les informations sont transmises et qu'elles soient ou non mises en cache ou stockées pendant la transmission, il convient de toujours protéger les informations de manière appropriée.

Les organismes de télécommunications et leurs systèmes d'information et réseaux sont exposés à des menaces de sécurité provenant de diverses sources, notamment : écoute en ligne ; cyberattaques persistantes ; terrorisme ; espionnage ; sabotage ; vandalisme ; fuite d'informations ; erreurs ; événements de force majeure. Ces menaces de sécurité peuvent trouver leur origine à l'intérieur ou à l'extérieur de l'organisme de télécommunications, entraînant un préjudice pour l'organisme.

Après une violation de la sécurité de l'information, par exemple par une écoute des lignes de télécommunications, l'organisme peut subir un préjudice. Il est par conséquent essentiel pour un organisme de garantir la sécurité de ses informations par une amélioration continue de son système de management de la sécurité de l'information (SMSI).

Une sécurité de l'information efficace est obtenue par la mise en œuvre d'un ensemble approprié de mesures fondées sur celles décrites dans la présente Recommandation | Norme internationale. Il est nécessaire d'établir, de mettre en œuvre, de surveiller, d'examiner et d'améliorer ces mesures dans les installations, services et applications de télécommunications. Ces activités permettront à un organisme d'atteindre ses objectifs de sécurité et, par conséquent, ses objectifs métier.

Les organismes de télécommunications fournissent à différents types d'utilisateur des installations pour traiter, transmettre et stocker les informations. Ces informations peuvent être des informations personnelles identifiables ou des données privées et métier confidentielles. Dans tous les cas, il convient de traiter les informations avec le niveau de soin et d'attention qui leur est dû, et de fournir les niveaux de protection appropriés pour en garantir la confidentialité, l'intégrité et la disponibilité (CID), en privilégiant par-dessus tout la vie privée et la sensibilité.

4.2.2 Considérations relatives à la sécurité dans les télécommunications

L'exigence d'un cadre générique pour la sécurité dans les télécommunications a été exprimée par différentes sources :

a) les clients/abonnés, qui ont besoin d'avoir confiance dans le réseau et les services fournis, y compris la disponibilité des services (en particulier les services d'urgence) en cas de catastrophes majeures ;

b) les autorités publiques qui, par des directives, lois et réglementations, exigent une forme de sécurité pour garantir la disponibilité des services, la concurrence loyale et la protection de la vie privée ;

c) les opérateurs de réseaux et les fournisseurs de services eux-mêmes, qui ont besoin d'une sécurité pour protéger leurs intérêts opérationnels et commerciaux, et pour honorer leurs obligations envers les clients et le public.

Il convient, par ailleurs, que les organismes de télécommunications tiennent compte des incidents de sécurité environnementaux et opérationnels ci-dessous.

a) Les services de télécommunications dépendent fortement de diverses installations interconnectées, telles que des routeurs, des commutateurs, des serveurs de noms de domaine, des systèmes de relais de transmission et un système de gestion de réseau (NMS). Des incidents de sécurité des télécommunications peuvent donc se produire sur divers équipements/installations, et les incidents peuvent se propager rapidement à travers le réseau dans d'autres équipements/installations.

b) Au-delà des installations de télécommunications, des vulnérabilités au niveau des protocoles et de la topologie de réseau peuvent également conduire à de graves incidents de sécurité. La convergence des réseaux filaires et sans fil peut notamment soulever des défis majeurs pour le développement de protocoles interopérables.

c) Les organismes de télécommunications sont fortement préoccupées par la possibilité d'une atteinte à la sécurité entraînant une indisponibilité du réseau. Une telle indisponibilité peut se révéler extrêmement coûteuse du point de vue des relations client, de la perte de revenus et des coûts de récupération. Des attaques délibérées visant la disponibilité de l'infrastructure nationale de télécommunications peuvent être perçues comme une préoccupation relevant de la sécurité nationale.

d) Les réseaux et systèmes de gestion des télécommunications sont susceptibles d'être la cible de pirates. Le vol de services de télécommunications constitue une motivation courante pour ce type d'attaque. Les vols de cette nature peuvent s'appuyer sur différentes techniques, notamment l'appel de fonctions de diagnostic, la manipulation de documents comptables, la modification de bases de données de provisionnement ou l'écoute d'appels d'abonnés.

e) Outre les intrusions externes, les opérateurs craignent que leur sécurité ne soit compromise par des sources externes, par exemple à la suite de modifications non valides des bases de données de gestion du réseau et des configurations de la part d'un personnel non autorisé. Ces incidents peuvent être accidentels ou délibérés.

f) Les services de télécommunications peuvent être perturbés par des programmes malveillants, tels que des vers et virus qui attaquent les systèmes finaux ou l'infrastructure de communications. Les attaques DoS/DDoS sont une cause majeure d'incidents de communications, et peuvent être perpétrées par diverses méthodes pour interrompre ou bloquer les signaux de communication, ou encore pour surcharger un système ou un réseau en lui envoyant des données simultanément depuis des centaines de systèmes (voir TEL 13.1.6).

Afin de protéger les actifs informationnels dans les télécommunications provenant de différentes sources dans divers environnements de télécommunications, des lignes directrices pour la sécurité des télécommunications sont indispensables pour encadrer la mise en œuvre de la gestion de la sécurité de l'information dans les organismes de télécommunications.

Il convient que les lignes directrices pour la sécurité s'appliquent :

a) aux organismes de télécommunications qui cherchent à avoir la garantie que les exigences en matière de sécurité de l'information exprimées par les parties intéressées (par exemple, fournisseurs, clients, législateurs) seront satisfaites ;

b) aux organismes de télécommunications qui cherchent à acquérir un avantage commercial par la mise en œuvre d'un SMSI ;

c) aux utilisateurs et fournisseurs de produits et services liés à la sécurité de l'information auprès du secteur des télécommunications ;

d) aux intervenants internes ou externes à l'organisme de télécommunications, qui évaluent et contrôlent la conformité du SMSI aux exigences de l'ISO/IEC 27001 ;

e) aux intervenants internes ou externes à l'organisme de télécommunications, qui dispensent des conseils ou des formations sur le SMSI adaptés à l'organisme ;

f) à la garantie de conformité aux exigences légales et réglementaires transfrontalières, et au respect des exigences légales dans tous les pays d'exploitation ou de transit.

4.2.3 Actifs à protéger

Afin d'établir la gestion de la sécurité de l'information, il est essentiel qu'un organisme clarifie et identifie l'ensemble de ses actifs organisationnels. La clarification des attributs et de l'importance des actifs rend possible la mise en œuvre de mesures appropriées.

Les actifs qu'il convient que les organismes de télécommunications protègent sont décrits au paragraphe 8.1.1.

4.2.4 Établissement d'une gestion de la sécurité de l'information

4.2.4.1 Modalités d'établissement des exigences de sécurité

Il est essentiel que les organismes de télécommunications identifient leurs exigences de sécurité. Ces exigences proviennent de trois sources principales :

a) celles dérivées de l'appréciation du risque pour un opérateur de télécommunications, compte tenu de sa stratégie globale et de ses objectifs généraux. L'appréciation du risque permet d'identifier les menaces pesant sur les actifs, d'analyser les vulnérabilités, de mesurer la vraisemblance des attaques et d'en évaluer l'impact potentiel ;

b) les exigences légales, statutaires, réglementaires et contractuelles que les organismes de télécommunications sont tenus de respecter, le respect des exigences légales et réglementaires transfrontalières et l'environnement socioculturel. La non-divulgation des communications (TEL.18.1.6, Annexe A) et la prise en charge des communications essentielles (TEL.18.1.7, Annexe A) sont des exemples d'exigences législatives applicables aux organismes de télécommunications. Les exigences socioculturelles consistent, par exemple, à garantir l'intégrité des télécommunications qui sont transmises, relayées et reçues par un quelconque moyen, la disponibilité des installations de télécommunications filaires ou sans fil par des personnes autorisées, et l'absence d'atteinte à d'autres installations de télécommunications ;

c) l'ensemble particulier de principes, d'objectifs et d'exigences métier en matière de traitement de l'information qu'un opérateur de télécommunications s'est constitué pour mener à bien ses activités.