NORME INTERNATIONALE

ISO/IEC 27017

Première édition
2015-12-15

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services



Numéro de référence
ISO/IEC 27017:2015(F)

© ISO/IEC 2015



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2015

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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

Publié en Suisse

Sommaire

Page

Avant-propos ..... **vii**

Introduction ..... **viii**

1 Domaine d'application **1**

2 Références normatives **1**

3 Termes, définitions et abréviations **1**
3.1 Termes et définitions 1
3.2 Abréviations 2

4 Concepts spécifiques au secteur du nuage **2**
4.1 Vue d'ensemble 2
4.2 Relations avec les fournisseurs dans les services en nuage 3
4.3 Relations entre les clients de services en nuage et les fournisseurs de services en nuage 3
4.4 Gestion des risques relatifs à la sécurité de l'information dans les services en nuage 4
4.5 Structure de la présente norme 4

5 Politiques de sécurité de l'information **5**
5.1 Orientations de la direction en matière de sécurité de l'information 5
5.1.1 Politiques de sécurité de l'information 5
5.1.2 Revue des politiques de sécurité de l'information 6

6 Organization de la sécurité de l'information **6**
6.1 Organization interne 6
6.1.1 Fonctions et responsabilités liées à la sécurité de l'information 6
6.1.2 Séparation des tâches 7
6.1.3 Relations avec les autorités 7
6.1.4 Relations avec des groupes de travail spécialisés 7
6.1.5 La sécurité de l'information dans la gestion de projet 7
6.2 Appareils mobiles et télétravail 7
6.2.1 Politique en matière d'appareils mobiles 7
6.2.2 Télétravail 8

7 Sécurité des ressources humaines **8**
7.1 Avant l'embauche 8
7.1.1 Sélection des candidats 8
7.1.2 Termes et conditions d'embauche 8
7.2 Pendant la durée du contrat 8
7.2.1 Responsabilités de la direction 8
7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information 8
7.2.3 Processus disciplinaire 9
7.3 Rupture, terme ou modification du contrat de travail 9
7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail 9

8 Gestion des actifs **9**
8.1 Responsabilités relatives aux actifs 9
8.1.1 Inventaire des actifs 9
8.1.2 Propriété des actifs 10
8.1.3 Utilization correcte des actifs 10
8.1.4 Restitution des actifs 10
8.2 Classification de l'information 10
8.2.1 Classification de l'information 10
8.2.2 Marquage des informations 10
8.2.3 Manipulation des actifs 11
8.3 Manipulation des supports 11
8.3.1 Gestion des supports amovibles 11
8.3.2 Mise au rebut des supports 11
8.3.3 Transfert physique des supports 11

© ISO/IEC 2015 – Tous droits réservés

9 Contrôle d'accès **11**
9.1 Exigences métier en matière de contrôle d'accès 11
9.1.1 Politique de contrôle d'accès 11
9.1.2 Accès aux réseaux et aux services en réseau 11
9.2 Gestion de l'accès utilizateur 12
9.2.1 Enregistrement et désinscription des utilizateurs 12
9.2.2 Maîtrise de la gestion des accès utilizateur 12
9.2.3 Gestion des privilèges d'accès 12
9.2.4 Gestion des informations secrètes d'authentification des utilizateurs 13
9.2.5 Revue des droits d'accès utilizateur 13
9.2.6 Suppression ou adaptation des droits d'accès 13
9.3 Responsabilités des utilizateurs 13
9.3.1 Utilization d'informations secrètes d'authentification 13
9.4 Contrôle de l'accès au système et aux applications 13
9.4.1 Restriction d'accès à l'information 14
9.4.2 Sécuriser les procédures de connexion 14
9.4.3 Système de gestion des mots de passe 14
9.4.4 Utilization de programmes utilitaires à privilèges 14
9.4.5 Contrôle d'accès au code source des programmes 14

10 Cryptographie **15**
10.1 Mesures cryptographiques 15
10.1.1 Politique d'utilization des mesures cryptographiques 15
10.1.2 Gestion des clés 15

11 Sécurité physique et environnementale **16**
11.1 Zones sécurisées 16
11.1.1 Périmètre de sécurité physique 16
11.1.2 Contrôles physiques des accès 16
11.1.3 Sécurisation des bureaux, des salles et des équipements 16
11.1.4 Protection contre les menaces extérieures et environnementales 16
11.1.5 Travail dans les zones sécurisées 17
11.1.6 Zones de livraison et de chargement 17
11.2 Matériels 17
11.2.1 Emplacement et protection du matériel 17
11.2.2 Services généraux 17
11.2.3 Sécurité du câblage 17
11.2.4 Maintenance du matériel 17
11.2.5 Sortie des actifs 17
11.2.6 Sécurité du matériel et des actifs hors des locaux 17
11.2.7 Mise au rebut ou recyclage sécurisé(e) du matériel 17
11.2.8 Matériel utilizateur laissé sans surveillance 18
11.2.9 Politique du bureau propre et de l'écran vide 18

12 Sécurité liée à l'exploitation **18**
12.1 Procédures et responsabilités liées à l'exploitation 18
12.1.1 Procédures d'exploitation documentées 18
12.1.2 Gestion des changements 18
12.1.3 Dimensionnement 19
12.1.4 Séparation des environnements de développement, de test et d'exploitation 19
12.2 Protection contre les logiciels malveillants 19
12.2.1 Mesures contre les logiciels malveillants 19
12.3 Sauvegarde 19
12.3.1 Sauvegarde des informations 20
12.4 Journalisation et surveillance 20
12.4.1 Journalisation des événements 20
12.4.2 Protection de l'information journalisée 21
12.4.3 Journaux administrateur et opérateur 21
12.4.4 Synchronisation des horloges 21
12.5 Maîtrise des logiciels en exploitation 22

 © ISO/IEC 2015 – Tous droits réservés

12.5.1 Installation de logiciels sur des systèmes en exploitation 22
12.6 Gestion des vulnérabilités techniques 22
12.6.1 Gestion des vulnérabilités techniques 22
12.6.2 Restrictions liées à l'installation de logiciels 22
12.7 Considérations sur l'audit des systèmes d'information 22
12.7.1 Mesures relatives à l'audit des systèmes d'information 23

13 Sécurité des communications 23
13.1 Management de la sécurité des réseaux 23
13.1.1 Contrôle des réseaux 23
13.1.2 Sécurité des services de réseau 23
13.1.3 Séparation des réseaux 23
13.2 Transfert de l'information 23
13.2.1 Politiques et procédures de transfert de l'information 23
13.2.2 Accords en matière de transfert d'information 24
13.2.3 Messagerie électronique 24
13.2.4 Engagements de confidentialité ou de non-divulgation 24

14 Acquisition, développement et maintenance des systèmes d'information 24
14.1 Exigences de sécurité applicables aux systèmes d'information 24
14.1.1 Analyse et spécification des exigences de sécurité de l'information 24
14.1.2 Sécurisation des services d'application sur les réseaux publics 24
14.1.3 Protection des transactions liées aux services d'application 24
14.2 Sécurité des processus de développement et d'assistance technique 25
14.2.1 Politique de développement sécurisé 25
14.2.2 Procédures de contrôle des changements apportés au système 25
14.2.3 Revue technique des applications après changement apporté à la plateforme d'exploitation 25
14.2.4 Restrictions relatives aux changements apportés aux progiciels 25
14.2.5 Principes d'ingénierie de la sécurité des systèmes 25
14.2.6 Environnement de développement sécurisé 25
14.2.7 Développement externalisé 25
14.2.8 Phase de test de la sécurité du système 26
14.2.9 Test de conformité du système 26
14.3 Données de test 26
14.3.1 Protection des données de test 26

15 Relations avec les fournisseurs 26
15.1 Sécurité de l'information dans les relations avec les fournisseurs 26
15.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs 26
15.1.2 La sécurité dans les accords conclus avec les fournisseurs 26
15.1.3 Chaîne d'approvisionnement informatique 27
15.2 Gestion de la prestation de services des fournisseurs 27
15.2.1 Surveillance et revue des services des fournisseurs 27
15.2.2 Gestion des changements apportés dans les services des fournisseurs 28

16 Gestion des incidents liés à la sécurité de l'information 28
16.1 Gestion des incidents liés à la sécurité de l'information et améliorations 28
16.1.1 Responsabilités et procédures 28
16.1.2 Signallement des événements liés à la sécurité de l'information 28
16.1.3 Signallement des failles liées à la sécurité de l'information 29
16.1.4 Appréciation des événements liés à la sécurité de l'information et prise de décision 29
16.1.5 Réponse aux incidents liés à la sécurité de l'information 29
16.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information 29
16.1.7 Recueil de preuves 29

17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité 30
17.1 Continuité de la sécurité de l'information 30
17.1.1 Organization de la continuité de la sécurité de l'information 30
17.1.2 Mise en œuvre de la continuité de la sécurité de l'information 30

© ISO/IEC 2015 – Tous droits réservés

17.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information 30
17.2 Redondances 30
17.2.1 Disponibilité des moyens de traitement de l'information 30

18 Conformité 30
18.1 Conformité aux obligations légales et contractuelles 30
18.1.1 Identification de la législation et des exigences contractuelles applicables 30
18.1.2 Droits de propriété intellectuelle 31
18.1.3 Protection des enregistrements 31
18.1.4 Protection de la vie privée et protection des données à caractère personnel 32
18.1.5 Réglementation relative aux mesures cryptographiques 32
18.2 Revue de la sécurité de l'information 32
18.2.1 Revue indépendante de la sécurité de l'information 32
18.2.2 Conformité avec les politiques et les normes de sécurité 33
18.2.3 Examen de la conformité technique 33

Annexe A (normative) **Ensemble étendu de mesures pour les services en nuage 34**

Annexe B (informative) **Références sur les risques de sécurité de l'information liés à l'informatique en nuage 39**

Bibliographie 41

 © ISO/IEC 2015 – Tous droits réservés

Avant-propos

L'ISO (Organization internationale de normalization) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalization 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'organization 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. 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 organismes nationaux 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.

L'ISO/IEC 27017 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*, en collaboration avec l'UIT-T. Le même texte est publié en tant que recommandation UIT-T. X.1631 (07/2015).

© ISO/IEC 2015 – Tous droits réservés

Introduction

Les lignes directrices contenues dans la présente Recommandation | Norme internationale viennent à l'appui et en complément des lignes directrices données dans l'ISO/IEC 27002.

Spécifiquement, cette Recommandation | Norme internationale fournit des lignes directrices appuyant la mise en œuvre des mesures de sécurité de l'information pour les clients et les fournisseurs de services en nuage. Certaines lignes directrices sont destinées aux clients des services du nuage qui ensurent la mise en œuvre des mesures, tandis que d'autres sont destinées aux fournisseurs de services en nuage afin de soutenir la mise en œuvre de ces mesures. Le choix approprié des mesures de sécurité de l'information et l'application des recommandations de mise en œuvre fournies dépendra d'une appréciation du risque et de toute exigence légale, contractuelle, réglementaire ou autre en matière de sécurité de l'information spécifique au secteur du nuage.

© ISO/IEC 2015 – Tous droits réservés

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

1 Domaine d'application

La présente Recommandation | Norme internationale contient des lignes directrices relatives aux mesures de sécurité de l'information applicables à la prestation et à l'utilization de services d'informatique en nuage, par exemple:

— des recommandations supplémentaires concernant la mise en œuvre des mesures de sécurité pertinentes spécifiées dans l'ISO/IEC 27002;

— des mesures de sécurité supplémentaires avec préconisations de mise en œuvre spécifiquement liées aux services en nuage.

La présente Recommandation | Norme internationale fournit des recommandations concernant les moyens de maîtrise et la mise en œuvre destinées aux prestataires de services d'informatique en nuage et à leurs clients.

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 normalization des télécommunications de l´UIT tient à jour une liste des Recommandations de l´UIT-T en vigueur.

Recommandation UIT-T Y 3500 (en vigueur) | ISO/IEC 17788: (en vigueur), *Technologies de l'information — Informatique en nuage — Vue d'ensemble et vocabulaire*

Recommandation UIT-T Y 3502 (en vigueur) | ISO/IEC 17789: (en vigueur), *Technologies de l'information — Informatique en nuage — Architecture de référence*

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 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins de la présente Recommandation | Norme internationale, les termes et définitions de l'ISO/IEC 27000, la Rec. UIT-T Y.3500 | l'ISO/IEC 17788, la Rec. UIT-T Y.3502 | l'ISO/IEC 17789 ainsi que les suivants, s'appliquent:

© ISO/IEC 2015 – Tous droits réservés

3.1.1
aptitude
qualité d'être capable d'accomplir une activité donnée.

3.1.2
violation de données
compromission de sécurité qui entraîne la destruction accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès à des données protégées transmises, stockées, ou soumises à un quelconque autre traitement;**multilocation sécurisée:** type de multilocation qui emploie des contrôles de sécurité pour une protection explicite contre les violations de données et qui produit la validation de ces contrôles pour une bonne gouvernance.

Note 1 à l'article: La multilocation sécurisée existe lorsque le profil de risque d'un locataire individuel n'est pas plus important qu'il ne le serait dans un environnement dédié à un seul locataire.

Note 2 à l'article: Dans les environnements très sécurisés, même l'identité des locataires est tenue secrète.

3.1.3
machine virtuelle
l'environnement complet qui supporte l'exécution des logiciels invités.

Note 1 à l'article: Une machine virtuelle est une encapsulation complète du matériel virtuel, des disques virtuels et des métadonnées qui y sont associées. Les machines virtuelles permettent le multiplexage de la machine physique sous-jacente par le biais d'une couche logicielle appelée hyperviseur.

3.2 Abréviations

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

DCP	Données à caractère personnel
IaaS	Infrastructure en tant que service (Infrastructure as a Service)
MV	machine virtuelle
PaaS	Plate-forme en tant que service (Platform as a Service)
SaaS	Logiciel en tant que service (Software as a Service)
SLA	Accord de niveau de service (Service Level Agreement)

4 Concepts spécifiques au secteur du nuage

4.1 Vue d'ensemble

L'utilization de l'informatique en nuage a modifié la façon dont il convient que les organismes apprécient et atténuent les risques liés à la sécurité de l'information en raison des changements importants dans la manière dont les ressources informatiques sont techniquement conçues, exploitées et gérées. La présente Recommandation | Norme internationale fournit des lignes directrices supplémentaires pour la mise en œuvre spécifique au nuage, fondées sur l'ISO/IEC 27002, et prévoit des mesures supplémentaires visant à traiter les considérations spécifiques au nuage en matière de menaces et les risques de sécurité des informations.

Il convient que les utilizateurs de la présente Recommandation | Norme internationale se réfèrent aux Articles 5 à 18 de l'ISO/IEC 27002 concernant les mesures, les préconisations de mise en œuvre et autres informations. En raison de l'applicabilité générale de l'ISO/IEC 27002, de nombreuses mesures, préconisations de mise en œuvre et autres informations s'appliquent à la fois au contexte général et au contexte de l'informatique en nuage d'un organisme. Par exemple, «6.1.2 Séparation des tâches» de

 © ISO/IEC 2015 – Tous droits réservés