

---

---

**Technologies de l'information —  
Techniques de sécurité — Gestion des  
risques liés à la sécurité de l'information**

*Information technology — Security techniques — Information security  
risk management*



**DOCUMENT PROTÉGÉ PAR COPYRIGHT**

© ISO/CEI 2011

Droits de reproduction réservés. Sauf prescription différente, 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 et les microfilms, sans l'accord écrit de l'ISO à l'adresse ci-après ou du comité membre de l'ISO dans le pays du demandeur.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Version française parue en 2013

Publié en Suisse

## Sommaire

Page

1	Domaine d'application .....	1
2	Références normatives .....	1
3	Termes et définitions .....	1
4	Structure de la présente Norme internationale .....	6
5	Contexte .....	6
6	Présentation générale du processus de gestion des risques en sécurité de l'information .....	7
7	Établissement du contexte .....	11
7.1	Considérations générales .....	11
7.2	Critères de base .....	12
7.2.1	Approche de gestion des risques .....	12
7.2.2	Critères d'évaluation du risque .....	12
7.2.3	Critères d'impact .....	12
7.2.4	Critères d'acceptation des risques .....	13
7.3	Domaine d'application et limites .....	13
7.4	Organisation de la gestion des risques en sécurité de l'information .....	14
8	Appréciation des risques en sécurité de l'information .....	15
8.1	Description générale de l'appréciation des risques en sécurité de l'information .....	15
8.2	Identification des risques .....	16
8.2.1	Introduction à l'identification des risques .....	16
8.2.2	Identification des actifs .....	16
8.2.3	Identification des menaces .....	17
8.2.4	Identification des mesures de sécurité existantes .....	17
8.2.5	Identification des vulnérabilités .....	18
8.2.6	Identification des conséquences .....	19
8.3	Analyse des risques .....	20
8.3.1	Méthodologies d'analyse des risques .....	20
8.3.2	Appréciation des conséquences .....	21
8.3.3	Appréciation de la vraisemblance d'un incident .....	22
8.3.4	Estimation du niveau des risques .....	23
8.4	Évaluation des risques .....	23
9	Traitement des risques en sécurité de l'information .....	24
9.1	Description générale du traitement des risques .....	24
9.2	Réduction du risque .....	26
9.3	Maintien des risques .....	28
9.4	Refus des risques .....	28
9.5	Partage des risques .....	28
10	Acceptation des risques en sécurité de l'information .....	28
11	Communication et concertation relatives aux risques en sécurité de l'information .....	29
12	Surveillance et revue du risque en sécurité de l'information .....	30
12.1	Surveillance et revue des facteurs de risque .....	30
12.2	Surveillance, revue et amélioration de la gestion des risques .....	31
<b>Annexe A (informative) Définition du domaine d'application et des limites du processus de gestion des risques en sécurité de l'information .....</b>		<b>33</b>
A.1	Étude de l'organisation .....	33
A.2	Liste des contraintes affectant l'organisation .....	34
A.3	Liste des références législatives et réglementaires applicables à l'organisation .....	36

**A.4 Liste des contraintes affectant le domaine d'application.....36**

**Annexe B (informative) Identification et valorisation des actifs et appréciation des impacts.....39**

**B.1 Exemples d'identification des actifs.....39**

**B.1.1 Identification des actifs primordiaux.....39**

**B.1.2 Liste et description des actifs en support .....40**

**B.2 Valorisation des actifs.....45**

**B.3 Appréciation des impacts .....48**

**Annexe C (informative) Exemples de menaces types .....50**

**Annexe D (informative) Vulnérabilités et méthodes d'appréciation des vulnérabilités .....52**

**D.1 Exemples de vulnérabilités.....52**

**D.2 Méthodes d'appréciation des vulnérabilités techniques.....55**

**Annexe E (informative) Approches d'appréciation des risques en sécurité de l'information.....57**

**E.1 Appréciation des risques de haut niveau en sécurité de l'information .....57**

**E.2 Appréciation détaillée des risques en sécurité de l'information .....58**

**E.2.1 Exemple 1 — Matrice avec valeurs prédéfinies.....59**

**E.2.2 Exemple 2 — Classement des menaces par mesures des risques.....61**

**E.2.3 Exemple 3 — Appréciation d'une valeur relative à la vraisemblance et aux conséquences  
possibles des risques .....62**

**Annexe F (informative) Contraintes liées à la réduction du risque.....64**

**Annexe G (informative) Différences de définitions entre l'ISO/CEI 27005:2008 et  
l'ISO/CEI 27005:2011 .....66**

**Bibliographie .....77**

## Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

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

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

L'attention est appelée 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 ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27005 a été élaborée par le comité technique ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette deuxième édition annule et remplace la première édition (ISO/CEI 27005:2008), qui a fait l'objet d'une révision technique.

## Introduction

La présente Norme internationale contient des lignes directrices relatives à la gestion des risques en sécurité de l'information dans une organisation, qui viennent notamment en appui des exigences d'un SMSI (système de management de la sécurité de l'information) tel que défini dans l'ISO/CEI 27001. Cependant, la présente Norme internationale ne fournit aucune méthodologie spécifique à la gestion des risques en sécurité de l'information. Il est du ressort de chaque organisation de définir son approche de la gestion des risques, en fonction, par exemple, du périmètre du SMSI, de ce qui existe dans l'organisation dans le domaine de la gestion des risques, ou encore de son secteur industriel. Plusieurs méthodologies existantes peuvent être utilisées en cohérence avec le cadre décrit dans la présente Norme internationale pour appliquer les exigences du SMSI.

La présente Norme internationale s'adresse aux responsables et aux personnels concernés par la gestion des risques en sécurité de l'information au sein d'une organisation et, le cas échéant, aux tiers prenant part à ces activités.

# Technologies de l'information — Techniques de sécurité — Gestion des risques en sécurité de l'information

## 1 Domaine d'application

La présente Norme internationale contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.

La présente Norme internationale vient en appui des concepts généraux énoncés dans l'ISO/CEI 27001; elle est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques.

Il est important de connaître les concepts, les modèles, les processus et les terminologies décrites dans l'ISO/CEI 27001 et l'ISO/CEI 27002 afin de bien comprendre la présente Norme internationale.

La présente Norme internationale est applicable à tous types d'organisations (par exemple les entreprises commerciales, les agences gouvernementales, les organisations à but non lucratif) qui ont l'intention de gérer des risques susceptibles de compromettre la sécurité des informations de l'organisation.

## 2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

ISO/CEI 27001:2005, *Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité de l'information — Exigences*

## 3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/CEI 27000 et les suivants s'appliquent.

NOTE Les différences de définitions entre l'ISO/CEI 27005:2008 et la présente Norme internationale sont indiquées dans l'Annexe G.

### 3.1

#### conséquence

effet d'un **événement** (3.3) affectant les objectifs

[Guide ISO 73:2009]

NOTE 1 Un événement unique peut engendrer des conséquences multiples.