

ICS: 35.040

---

# *Geregistreeerde Belgische norm*

## **NBN ISO/IEC 27002/AC**

1e uitg., november 2014

**Normklasse: Z 07**

---

### **Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (ISO/IEC 27002/Cor1:2014)**

Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002/Cor1:2014)

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information ISO/IEC 27002/Cor1:2014)

---

**Toelating tot publicatie: 28 november 2014**

Dit corrigendum is van toepassing op de norm NBN ISO/IEC 27002 (2014).



**Bureau voor Normalisatie - Jozef II-straat 40 - 1000 Brussel - België**

Tel: +32 2 738 01 12 - Fax: +32 2 733 42 64 - E-mail: [info@nbn.be](mailto:info@nbn.be) - NBN Online: [www.nbn.be](http://www.nbn.be)  
Bank 000-3255621-10 IBAN BE41 0003 2556 2110 BIC BPOTBEB1 BTW BE0880857592

ICS: 35.040

---

*norme belge  
enregistrée*

**NBN ISO/IEC 27002/AC**

1e éd., novembre 2014

**Indice de classement: Z 07**

---

**Information technology - Security techniques - Code of practice for  
information security controls (ISO/IEC 27002/Cor1:2014)**

Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (ISO/IEC 27002/Cor1:2014)

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information ISO/IEC 27002/Cor1:2014)

---

**Autorisation de publication: 28 novembre 2014**

Le présent corrigendum s'applique à la norme NBN ISO/IEC 27002 (2014).



**Bureau de Normalisation - rue Joseph II 40 - 1000 Bruxelles - Belgique**

Tél: +32 2 738 01 12 - Fax: +32 2 733 42 64 - E-mail: [info@nbn.be](mailto:info@nbn.be) - NBN Online: [www.nbn.be](http://www.nbn.be)  
Banque 000-3255621-10 IBAN BE41 0003 2556 2110 BIC BPOTBEB1 TVA BE0880857592



NBN ISO\_IEC 27002/AC (2014)

**INTERNATIONAL STANDARD ISO/IEC 27002:2013**

**TECHNICAL CORRIGENDUM 1**

Published 2014-09-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION  
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

# **Information technology — Security techniques — Code of practice for information security controls**

## **TECHNICAL CORRIGENDUM 1**

*Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

*RECTIFICATIF TECHNIQUE 1*

Technical Corrigendum 1 to ISO/IEC 27002:2013 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*



# Information technology — Security techniques — Code of practice for information security controls

## Technical corrigendum 1

Technical Corrigendum 1 to ISO/IEC 27002:2013 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, Security techniques.

Page 10, Subclause 7.1.2

Replace

### Implementation Guidance

.....

c) responsibilities for the classification of information and management of organizational assets associated with information, information processing facilities and information services handled by the employee or contractor (see Clause 8)

with

### Implementation Guidance

.....

c) responsibilities for the classification of information and management of organizational information, other assets associated with information, information processing facilities and information services handled by the employee or contractor (see Clause 8)

Page 13, Subclause 8.1.1

Replace

### Control

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

with

### Control

Information, other assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

Page 14, Subclause 8.1.3

Replace

Implementation Guidance

Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources.

with

Implementation Guidance

Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's information, other assets associated with information and information processing facilities and resources.

