



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*

Copyright International Organization for standardization ISO- Geneva- Switzerland.  
All rights reserved. This copy has been made by BSB Edge Pvt. Ltd. with the permission from ISO. No resale of this document is permitted. No part of this document may be copied or reproduced in any form by any means (graphic- electronic or mechanical- including photocopying- recording- retrieval system)- nor made available on the internet or any public network without the prior written consent of ISO.

ICS 35.040

Ref. No. ISO/IEC 27002:2013/Cor.1:2014(E)

© ISO/IEC 2014 – All rights reserved

Published in Switzerland



# 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.

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.



# INTERNATIONAL STANDARD ISO/IEC 27002:2013 TECHNICAL CORRIGENDUM 2

Published 2015-11-15

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 2

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

*RECTIFICATIF TECHNIQUE 2*

Technical Corrigendum 2 to ISO/IEC 27002:2013 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*

Copyright International Organization for standardization ISO- Geneva- Switzerland.  
All rights reserved. This copy has been made by BSB Edge Pvt. Ltd. with the permission from ISO. No resale of this document is permitted. No part of this document may be copied or reproduced in any form by any means (graphic- electronic or mechanical- including photocopying- recording- retrieval system)- nor made available on the internet or any public network without the prior written consent of ISO.

Page 61, Subclause 14.2.8

*Replace*

Implementation Guidance

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected (see 14.1.1 and 14.1.9). The extent of testing should be in proportion to the importance and nature of the system.

*With*

Implementation Guidance

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected (see 14.1.1 and 14.2.9). The extent of testing should be in proportion to the importance and nature of the system.