NSAI
Standards

Irish Standard
I.S. ISO/IEC 27002:2013

Information technology -- Security techniques -- Code of practice for information security controls & Technical Corrigenda 1 & 2

I.S. ISO/IEC 27002:2013

Incorporating amendments/corrigenda/National Annexes issued since publication:
ISO/IEC 27002:2013/AC1:2014
ISO/IEC 27002:2013/AC2:2015

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard – national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation - recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces:	*This document is based on:* ISO/IEC 27002:2013	*Published:* 12 January, 2016

This document was published under the authority of the NSAI and comes into effect on: 12 January, 2016	ICS number: 35.040

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W **NSAI.ie**

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

DECLARATION

OF

SPECIFICATION

INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

& TECHNICAL CORRIGENDA 1 & 2

AS

THE IRISH STANDARD SPECIFICATION FOR

INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

& TECHNICAL CORRIGENDA 1 & 2

_____

NSAI in exercise of the power conferred by section 16 (5) of the National Standards Authority of Ireland Act, 1996 (No. 28 of 1996) and with the consent of the Minister for Jobs, Enterprise and Innovation, hereby declare as follows:

1.   This instrument may be cited as the Standard Specification (Information technology -- Security techniques -- Code of practice for information security controls & Technical Corrigenda 1 & 2) Declaration, 2016.

2.   (1) The Specification set forth in the Schedule to this declaration is hereby declared to be the standard specification for Information technology -- Security techniques -- Code of practice for information security controls & Technical Corrigenda 1 & 2.

   (2) The said standard specification may be cited as Irish Standard ISO/IEC 27002:2013 or as I.S. ISO/IEC 27002:2013.

This page is intentionally left BLANK.

I.S. ISO/IEC 27002:2013
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*

_____

ICS 35.040   **Ref. No. ISO/IEC 27002:2013/Cor.2:2015(E)**

Published in Switzerland

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.