BS EN ISO/IEC 27041:2016

BSI Standards Publication

Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method (ISO/IEC 27041:2015)

bsi.

AVA Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27041:2016

National foreword

This British Standard is the UK implementation of EN ISO/IEC 27041:2016. It is identical to ISO/IEC 27041:2015. It supersedes BS ISO/IEC 27041:2015 which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee IST/33, IT - Security techniques, to Subcommittee IST/33/4, Security Controls and Services.

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 83393 9

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2015.

Amendments/corrigenda issued since publication

Date	Text affected
30 September 2016	This corrigendum renumbers BS ISO/IEC 27041:2015 as BS EN ISO/IEC 27041:2016.

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27041:2016

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 27041

August 2016

ICS 35.040

English Version

Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method (ISO/IEC 27041:2015)

Technologies de l'information - Techniques de sécurité - Directives sur la façon d'assurer l'aptitude à l'emploi et l'adéquation d'une méthode d'investigation d'incident (ISO/IEC 27041:2015)

Informationstechnik - IT-Sicherheitsverfahren - Leitfaden zur Sicherung der Tauglichkeit und Eignung von Vorfall-Untersuchungsmethoden (ISO/IEC 27041:2015)

This European Standard was approved by CEN on 19 June 2016.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2016 CEN and CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN and CENELEC national Members.

Ref. No. EN ISO/IEC 27041:2016 E

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27041:2016

European foreword

The text of ISO/IEC 27041:2015 has been prepared by Technical Committee Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27041:2016.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2017, and conflicting national standards shall be withdrawn at the latest by February 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27041:2015 has been approved by CEN as EN ISO/IEC 27041:2016 without any modification.

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27041:2016

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Symbols and abbreviated terms ... **4**

5 Method development and assurance ... **4**
- 5.1 Overview ... 4
- 5.2 General principles ... 4
- 5.3 General development and deployment model ... 4
- 5.4 Assurance stages ... 5
- 5.5 Requirements capture and analysis ... 6
  - 5.5.1 General principles of requirements ... 6
  - 5.5.2 Functional Requirements ... 7
  - 5.5.3 Verification of requirements ... 7
- 5.6 Process Design ... 7
  - 5.6.1 Overview ... 7
  - 5.6.2 Tool Selection ... 7
  - 5.6.3 Uncertainty and risk evaluation ... 7
- 5.7 Process Implementation ... 8
  - 5.7.1 Overview ... 8
  - 5.7.2 Tool choice — guidance for deployment ... 8
- 5.8 Process Verification ... 8
  - 5.8.1 General principles of verification ... 8
  - 5.8.2 Verification of processes ... 9
  - 5.8.3 Verification of tools ... 9
- 5.9 Process Validation ... 9
  - 5.9.1 General principles of validation ... 9
  - 5.9.2 Comprehensive validation ... 9
  - 5.9.3 Sufficient validation ... 9
  - 5.9.4 Fully validated processes ... 10
  - 5.9.5 Failed validation ... 10
- 5.10 Confirmation ... 10
- 5.11 Deployment ... 10
  - 5.11.1 Tool choice ... 10
- 5.12 Review and Maintenance ... 10

6 Assurance Models ... **11**
- 6.1 Overview ... 11
- 6.2 In-house assurance ... 11
- 6.3 External assurance ... 11
- 6.4 Mixed assurance ... 11

7 Production of evidence for assurance ... **11**
- 7.1 Overview ... 11
- 7.2 Pre-validation preparation ... 12
- 7.3 Producing Evidence of Validation ... 12
- 7.4 Maintenance of Validation ... 12
- 7.5 Validation of Examinations ... 12
- 7.6 Validation of Investigations ... 13

Annex A (informative) **Examples** ... **14**

Bibliography ... **18**

Documents
Document Sharing Hub

© ISO/IEC 2015 – All rights reserved

Full document details: BS EN ISO/IEC 27041:2016

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27041:2016

Introduction

About this International Standard

This International Standard is concerned with providing assurance that the investigative process used is appropriate for the incident under investigation and the results which are required. It also describes, at an abstract level, the concept of breaking seemingly complex processes into a series of smaller atomic parts, which should aid in the development of simple, yet robust, investigation methods. It should be considered by any person authorising, giving instruction for, managing, or conducting an investigation. It should be applied prior to any investigation, in the context of principles and processes (defined in ISO/IEC 27043:2015) and sound preparation and planning (defined in ISO/IEC 27035-2[1)]) to ensure the suitability of methods to be applied in the investigative processes described in ISO/IEC 27037:2012 and ISO/IEC 27042:2015.

Relationship to other standards

This International Standard is intended to complement other standards and documents which give guidance on the investigation of, and preparation to investigate, information security incidents. It is not a comprehensive guide, but lays down certain fundamental principles which are intended to ensure that tools, techniques, and methods can be selected appropriately and shown to be fit for purpose should the need arise.

This International Standard also intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyse, and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

This International Standard describes part of a comprehensive investigative process which includes, but is not limited to, the following topic areas:

— incident management, including preparation and planning for investigations;

— handling of digital evidence;

— use of, and issues caused by, redaction;

— intrusion prevention and detection systems, including information which can be obtained from these systems;

— security of storage, including sanitization of storage;

— ensuring that investigative methods are fit for purpose;

— carrying out analysis and interpretation of digital evidence;

— understanding principles and processes of digital evidence investigations;

— security incident event management, including derivation of evidence from systems involved in security incident event management;

— relationship between electronic discovery and other investigative methods, as well as the use of electronic discovery techniques in other investigations;

— governance of investigations, including forensic investigations.

These topic areas are addressed, in part, by the following ISO/IEC standards:

— ISO/IEC 27037:2012

1) To be published.

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27041:2016

This International Standard describes the means by which those involved in the early stages of an investigation, including initial response, can ensure that sufficient potential digital evidence is captured to allow the investigation to proceed appropriately.

— ISO/IEC 27038:2014

Some documents can contain information that must not be disclosed to some communities. Modified documents can be released to these communities after an appropriate processing of the original document. The process of removing information that is not to be disclosed is called "redaction".

The digital redaction of documents is a relatively new area of document management practice, raising unique issues and potential risks. Where digital documents are redacted, removed information must not be recoverable. Hence, care needs to be taken so that redacted information is permanently removed from the digital document (e.g. it must not be simply hidden within non-displayable portions of the document).

ISO/IEC 27038:2014 specifies methods for digital redaction of digital documents. It also specifies requirements for software that can be used for redaction.

— ISO/IEC 27040:2015

This International Standard provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.

Security mechanisms like encryption and sanitization can affect one's ability to investigate by introducing obfuscation mechanisms. They have to be considered prior to and during the conduct of an investigation. They can also be important in ensuring that storage of evidential material during and after an investigation is adequately prepared and secured.

— ISO/IEC 27042:2015

This International Standard describes how methods and processes to be used during an investigation can be designed and implemented in order to allow correct evaluation of potential digital evidence, interpretation of digital evidence, and effective reporting of findings.

— ISO/IEC 27043:2015

This International Standard defines the key common principles and processes underlying the investigation of incidents and provides a framework model for all stages of investigations.

The following ISO/IEC projects also address, in part, the topic areas identified above and can lead to the publication of relevant standards at some time after the publications of this International Standard.

— ISO/IEC 27035 (all parts)[2)]

This is a three-part standard that provides organizations with a structured and planned approach to the management of security incident management. It is composed of

— ISO/IEC 27035-1[3)]

2) To be published.

3) To be published.

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27041:2016

This part presents basic concepts and phases of information security incident management. It combines these concepts with principles in a structured approach to detecting, reporting, assessing, responding, and applying lessons learned.

— ISO/IEC 27035-2[4)]

This part presents the concepts to plan and prepare for incident response. The concepts, including incident management policy and plan, incident response team establishment, and awareness briefing and training, are based on the plan and prepare phase of the model presented in ISO/IEC 27035-1[5)]. This part also covers the "Lessons Learned" phase of the model.

— ISO/IEC 27035-3[6)]

This part includes staff responsibilities and practical incident response activities across the organization. Particular focus is given to the incident response team activities such including monitoring, detection, analysis, and response activities for the collected data or security events.

— ISO/IEC 27050 (all parts)[7)]

This addresses activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of electronically stored information (ESI). In addition, it provides guidance on measures, spanning from initial creation of ESI through its final disposition, which an organization can undertake to mitigate risk and expense should electronic discovery become an issue. It is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities. It is important to note that this guidance is not intended to contradict or supersede local jurisdictional laws and regulations.

Electronic discovery often serves as a driver for investigations, as well as evidence acquisition and handling activities. In addition, the sensitivity and criticality of the data sometimes necessitate protections like storage security to guard against data breaches.

— ISO/IEC 30121:2015

This International Standard provides a framework for governing bodies of organizations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organization for digital investigations before they occur. This International Standard applies to the development of strategic processes (and decisions) relating to the retention, availability, access, and cost effectiveness of digital evidence disclosure. This International Standard is applicable to all types and sizes of organizations. The International Standard is about the prudent strategic preparation for digital investigation of an organization. Forensic readiness ensures that an organization has made the appropriate and relevant strategic preparation for accepting potential events of an evidential nature. Actions may occur as the result of inevitable security breaches, fraud, and reputation assertion. In every situation, information technology (IT) has to be strategically deployed to maximize the effectiveness of evidential availability, accessibility, and cost efficiency

Figure 1 shows typical activities surrounding an incident and its investigation. The numbers shown in this diagram (e.g. 27037) indicate the International Standards listed above and the shaded bars show where each is most likely to be directly applicable or has some influence over the investigative process (e.g. by setting policy or creating constraints). It is recommended, however, that all should be consulted prior to, and during, the planning and preparation phases. The process classes shown are defined fully in this International Standard and the activities identified match those discussed in more detail in ISO/IEC 27035-2, ISO/IEC 27037:2012, and ISO/IEC 27042:2015.

---

4) To be published.

5) To be published.

6) To be published.

7) New project.

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27041:2016

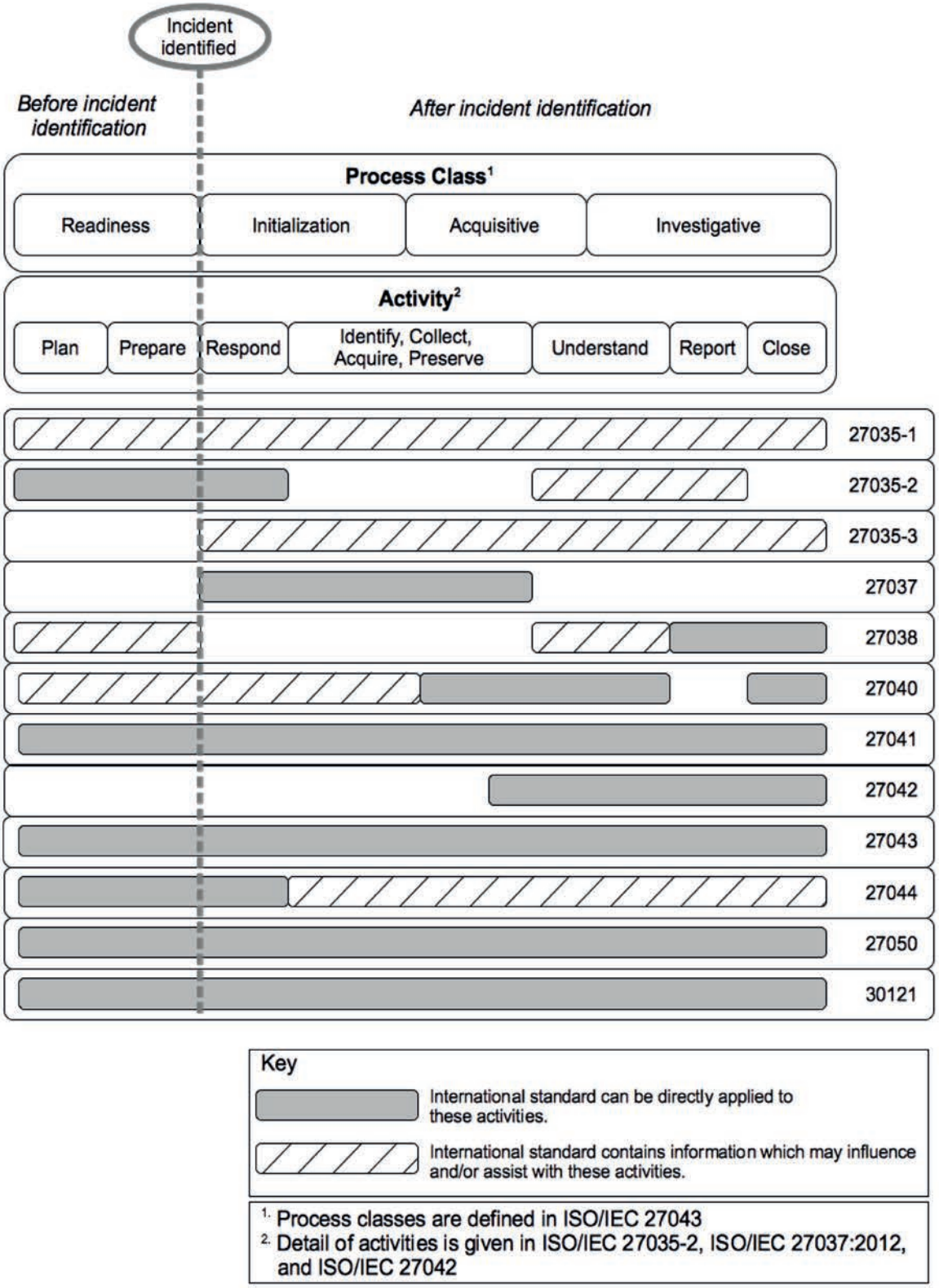

Figure 1 — Applicability of standards to investigation process classes and activities

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27041:2016