BS EN ISO/IEC 27043:2016

BSI Standards Publication

# Information technology — Security techniques — Incident investigation principles and processes (ISO/IEC 27043:2015)

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27043:2016

## National foreword

This British Standard is the UK implementation of EN ISO/IEC 27043:2016. It is identical to ISO/IEC 27043:2015. It supersedes BS ISO/IEC 27043:2015 which is withdrawn.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 92355 5

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 31 March 2015.

**Amendments/corrigenda issued since publication**

| Date | Text affected |
|---|---|
| 30 September 2016 | This corrigendum renumbers BS ISO/IEC 27043:2015 as BS EN ISO/IEC 27043:2016 |

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27043:2016

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN ISO/IEC 27043

August 2016

ICS 35.040

English Version

# Information technology - Security techniques - Incident investigation principles and processes (ISO/IEC 27043:2015)

Technologies de l'information - Techniques de sécurité - Principes d'investigation numérique et les processus (ISO/IEC 27043:2015)

Informationstechnik - IT-Sicherheitsverfahren - Grundsätze und Prozesse für die Untersuchung von Vorfällen (ISO/IEC 27043:2015)

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 27043:2016 E

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27043:2016

## European foreword

The text of ISO/IEC 27043:2015 has been prepared by Technical 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 27043:2016.

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 27043:2015 has been approved by CEN as EN ISO/IEC 27043:2016 without any modification.

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27043:2016

**Foreword** ... v
**Introduction** ... vi
**1 Scope** ... 1
**2 Normative references** ... 1
**3 Terms and definitions** ... 1
**4 Symbols and abbreviated terms** ... 3
**5 Digital investigations** ... 4
5.1 General principles ... 4
5.2 Legal principles ... 4
**6 Digital investigation processes** ... 5
6.1 General overview of the processes ... 5
6.2 Classes of digital investigation processes ... 5
**7 Readiness processes** ... 7
7.1 Overview of the readiness processes ... 7
7.2 Scenario definition process ... 9
7.3 Identification of potential digital evidence sources process ... 9
7.4 Planning pre-incident gathering, storage, and handling of data representing potential digital evidence process ... 11
7.5 Planning pre-incident analysis of data representing potential digital evidence process ... 11
7.6 Planning incident detection process ... 11
7.7 Defining system architecture process ... 11
7.8 Implementing system architecture process ... 12
7.9 Implementing pre-incident gathering, storage, and handling of data representing potential digital evidence process ... 12
7.10 Implementing pre-incident analysis of data representing potential digital evidence process ... 12
7.11 Implementing incident detection process ... 12
7.12 Assessment of implementation process ... 13
7.13 Implementation of assessment results process ... 13
**8 Initialization processes** ... 13
8.1 Overview of initialization processes ... 13
8.2 Incident detection process ... 14
8.3 First response process ... 15
8.4 Planning process ... 15
8.5 Preparation process ... 15
**9 Acquisitive processes** ... 16
9.1 Overview of acquisitive processes ... 16
9.2 Potential digital evidence identification process ... 16
9.3 Potential digital evidence collection process ... 17
9.4 Potential digital evidence acquisition process ... 17
9.5 Potential digital evidence transportation process ... 17
9.6 Potential digital evidence storage and preservation process ... 17
**10 Investigative processes** ... 18
10.1 Overview of investigative processes ... 18
10.2 Potential digital evidence acquisition process ... 19
10.3 Potential digital evidence examination and analysis process ... 19
10.4 Digital evidence interpretation process ... 19
10.5 Reporting process ... 19
10.6 Presentation process ... 20
10.7 Investigation closure process ... 20

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27043:2016

**11 Concurrent processes** ..... **20**
11.1 Overview of the concurrent processes ..... 20
11.2 Obtaining authorization process ..... 21
11.3 Documentation process ..... 21
11.4 Managing information flow process ..... 21
11.5 Preserving chain of custody process ..... 21
11.6 Preserving digital evidence process ..... 22
11.7 Interaction with physical investigation process ..... 22
**12 Digital investigation process model schema** ..... **22**
**Annex A** (informative) **Digital investigation processes: motivation for harmonization** ..... **24**
**Bibliography** ..... **28**


© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27043:2016

# 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*, Subcommittee SC 27, *Security techniques*.

© ISO/IEC 2015 – All rights reserved


Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27043:2016

# Introduction

## About this International Standard

This International Standard provides guidelines that encapsulate idealized models for common investigation processes across various investigation scenarios. This includes processes from pre-incident preparation up to and including returning evidence for storage or dissemination, as well as general advice and caveats on processes and appropriate identification, collection, acquisition, preservation, analysis, interpretation, and presentation of evidence. A basic principle of digital investigations is repeatability, where a suitably skilled investigator has to be able to obtain the same result as another similarly skilled investigator, working under similar conditions. This principle is exceptionally important to any general investigation. Guidelines for many investigation processes have been provided to ensure that there is clarity and transparency in obtaining the produced result for each particular process. The motivation to provide guidelines for incident investigation principles and processes follows.

Established guidelines covering incident investigation principles and processes would expedite investigations because they would provide a common order of the events that an investigation entails. Using established guidelines allows smooth transition from one event to another during an investigation. Such guidelines would also allow proper training of inexperienced investigators. The guidelines, furthermore, aim to assure flexibility within an investigation due to the fact that many different types of digital investigations are possible. Harmonized incident investigation principles and processes are specified and indications are provided of how the investigation processes can be customized in different investigation scenarios.

A harmonized investigation process model is needed in criminal and civil prosecution settings, as well as in other environments, such as corporate breaches of information security and recovery of digital information from a defective storage device. The provided guidelines give succinct guidance on the exact process to be followed during any kind of digital investigation in such a way that, if challenged, no doubt should exist as to the adequacy of the investigation process followed during such an investigation.

Any digital investigation requires a high level of expertise. Those involved in the investigation have to be competent, proficient in the processes used, and they have to use validated processes (see ISO/IEC 27041) which are compatible with the relevant policies and/or laws in applicable jurisdictions.

Where the need arises to assign a process to a person, that person will take the responsibility for the process. Therefore, a strong correlation between a process responsibility and a person's input will determine the exact investigation process required according to the harmonized investigation processes provided as guidelines in this International Standard.

This International Standard is structured by following a top-down approach. This means that the investigation principles and processes are first presented on a high (abstract) level before they are refined with more details. For example, a high-level overview of the investigation principles and processes are provided and presented in figures as "black boxes" at first, where after each of the high-level processes are divided into more fine-grained (atomic) processes. Therefore, a less abstract and more detailed view of all the investigation principles and processes are presented near the end of this International Standard as shown in Figure 8.

This International Standard is intended to complement other standards and documents which provide guidance on the investigation of, and preparation to, investigate information security incidents. It is not an in-depth guide, but it is a guide that provides a rather wide overview of the entire incident investigation process. This guide also 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.

## 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


© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27043:2016

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

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

— ISO/IEC 27038

  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 specifies methods for digital redaction of digital documents. It also specifies requirements for software that can be used for redaction.

— ISO/IEC 27040

  This International Standard provides detailed technical guidance on how organizations may define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the

AVA Documents
Document Sharing Hub

© ISO/IEC 2015 – All rights reserved


Full document details: BS EN ISO/IEC 27043:2016

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 27041

It is important that methods and processes deployed during an investigation can be shown to be appropriate. This document provides guidance on how to provide assurance that methods and processes meet the requirements of the investigation and have been appropriately tested.

— ISO/IEC 27042

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.

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)

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

— ISO/IEC 27035-2

— ISO/IEC 27035-3

— ISO/IEC 27044

— ISO/IEC 27050 (all parts)

— ISO/IEC 30121

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 assures 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


© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27043:2016

in this International Standard and the activities identified match those discussed in more detail in ISO/IEC 27035-2, ISO/IEC 27037, and ISO/IEC 27042.

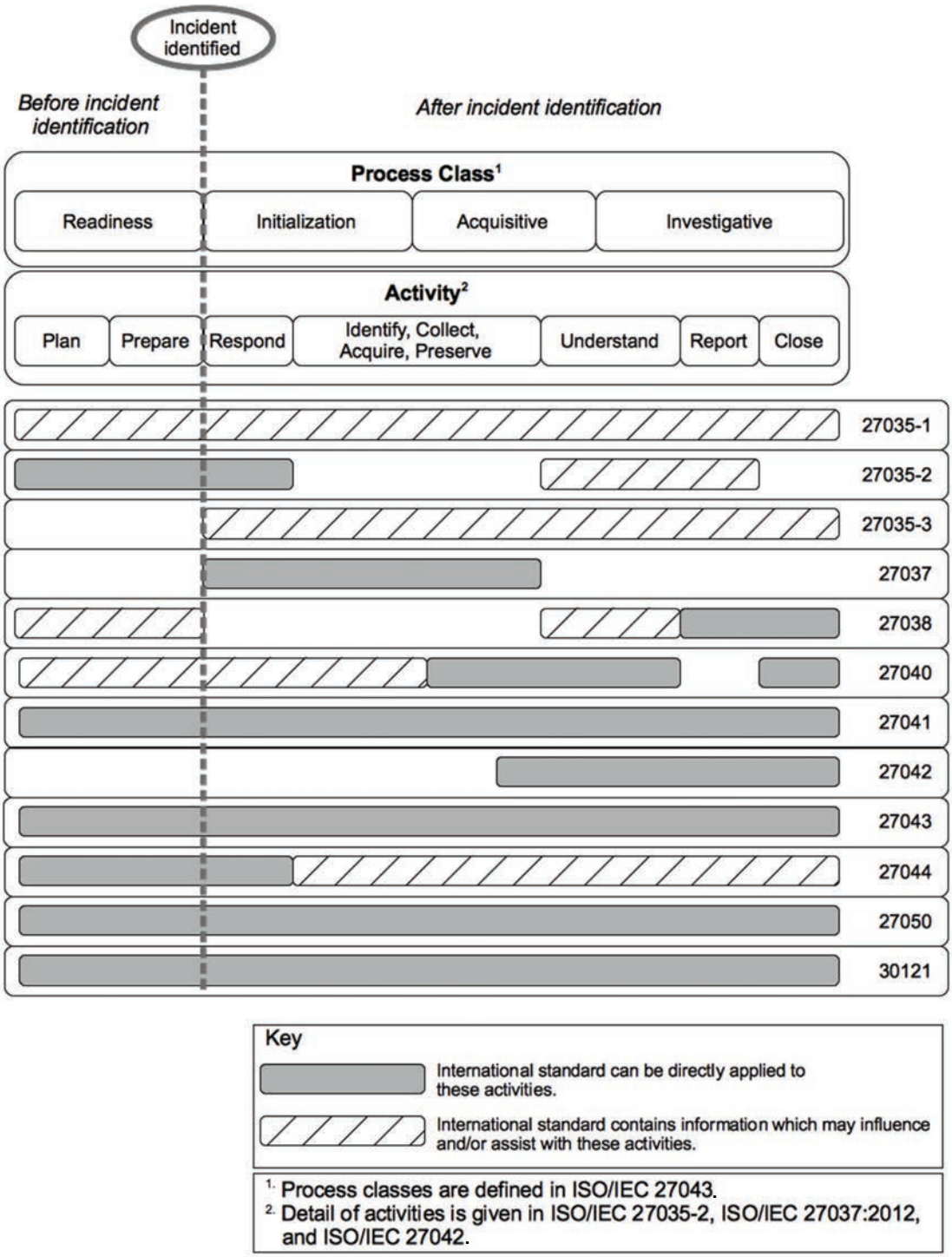


**Figure 1 — Applicability of standards to investigation process classes and activities**

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27043:2016

Documents
Document Sharing Hub

# Information technology — Security techniques — Incident investigation principles and processes

## 1 Scope

This International Standard provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence. This includes processes from pre-incident preparation through investigation closure, as well as any general advice and caveats on such processes. The guidelines describe processes and principles applicable to various kinds of investigations, including, but not limited to, unauthorized access, data corruption, system crashes, or corporate breaches of information security, as well as any other digital investigation.

In summary, this International Standard provides a general overview of all incident investigation principles and processes without prescribing particular details within each of the investigation principles and processes covered in this International Standard. Many other relevant International Standards, where referenced in this International Standard, provide more detailed content of specific investigation principles and processes.

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

**3.1**
**acquisition**
process of creating a copy of data within a defined set

Note 1 to entry: The product of an acquisition is a potential digital evidence copy.

[SOURCE: ISO/IEC 27037:2012, 3.1]

**3.2**
**activity**
set of cohesive tasks of a process

[SOURCE: ISO/IEC 12207:2008, 4.3]

**3.3**
**analysis**
process of evaluating potential digital evidence in order to assess its relevance to the investigation

Note 1 to entry: Potential digital evidence, which is determined to be relevant, becomes digital evidence.

[SOURCE: ISO/IEC 27042:—, 3.1]

© ISO/IEC 2015 – All rights reserved



Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27043:2016

**3.4**
**collection**
process of gathering the physical items that contain potential digital evidence

[SOURCE: ISO/IEC 27037:2012, 3.3]

**3.5**
**digital evidence**
information or data, stored or transmitted in binary form, that may be relied on as evidence

[SOURCE: ISO/IEC 27037:2012, 3.5]

**3.6**
**digital investigation**
use of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation, distribution, return, and/or destruction of digital evidence derived from digital sources, while obtaining proper authorizations for all activities, properly documenting all activities, interacting with the physical investigation, preserving digital evidence, and maintaining the chain of custody, for the purpose of facilitating or furthering the reconstruction of events found to be incidents requiring a digital investigation, whether of criminal nature or not

**3.7**
**identification**
process involving the search for, recognition, and documentation of potential digital evidence

[SOURCE: ISO/IEC 27037:2012, 3.12]

**3.8**
**incident**
single or a series of unwanted or unexpected information security breaches or events, whether of criminal nature or not, that have a significant probability of compromising business operations or threatening information security

**3.9**
**interpretation**
synthesis of an explanation, within agreed limits, for the factual information about evidence resulting from the set of examinations and analysis making up the investigation

[SOURCE: ISO/IEC 27042:—, 3.9]

**3.10**
**investigation**
application of examinations, analysis, and interpretation to aid understanding of an incident

[SOURCE: ISO/IEC 27042:—, 3.10]

**3.11**
**method**
definition of an operation which can be used to produce data or derive information as an output from specified inputs

Note 1 to entry: Ideally, a method should be atomic (i.e. it should not perform more than one function) in order to promote re-use of methods and the processes derived from them and to reduce the amount of work required to validate processes.

[SOURCE: ISO/IEC 27041:—, 3.11]


© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27043:2016