INTERNATIONAL STANDARD

ISO/IEC 27041

First edition
2015-06-15

Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method

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

Reference number
ISO/IEC 27041:2015(E)

© ISO/IEC 2015

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

© ISO/IEC 2015 – All rights reserved

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

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

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

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

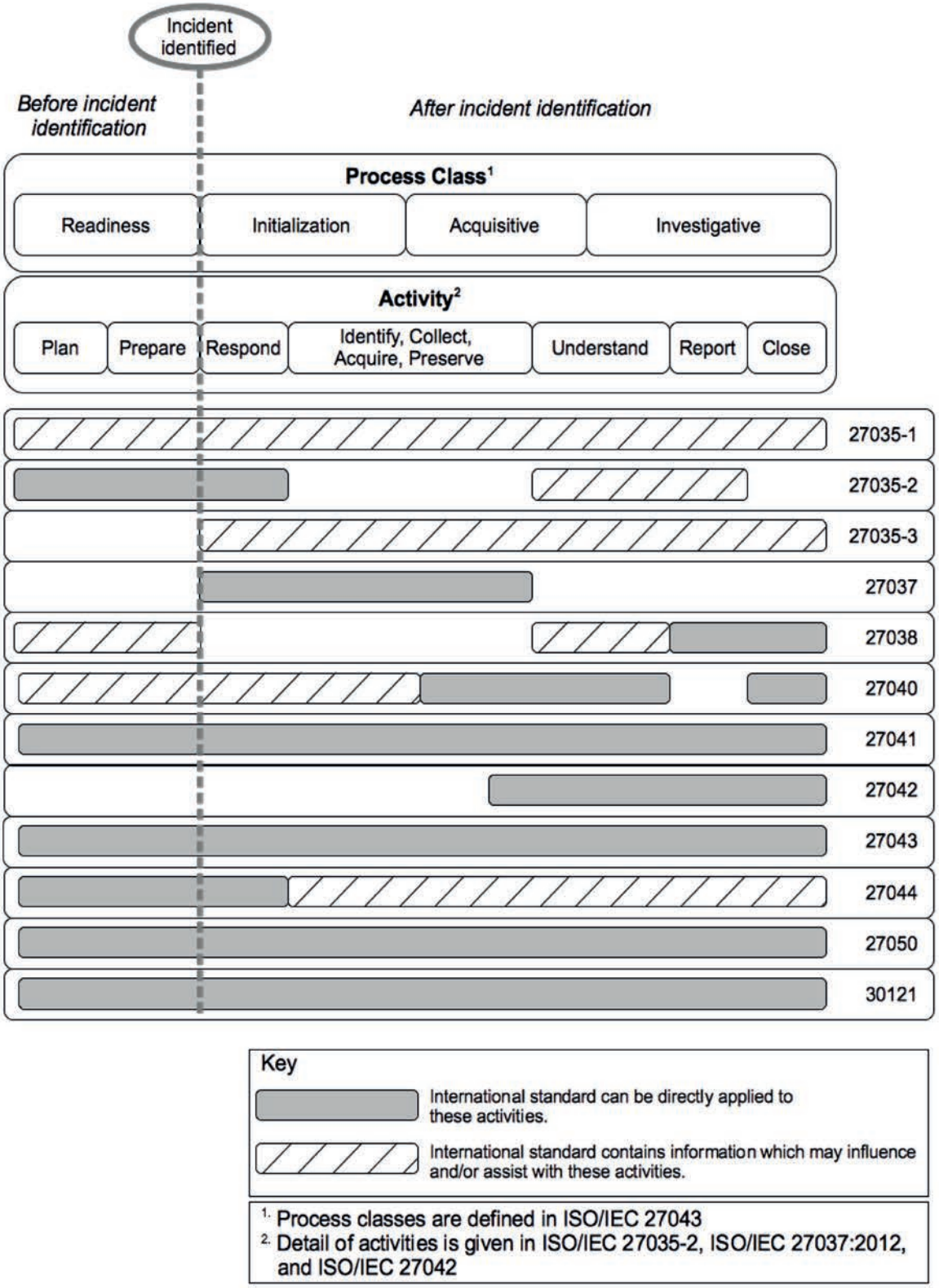

Figure 1 — Applicability of standards to investigation process classes and activities

© ISO/IEC 2015 – All rights reserved

Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method

1 Scope

This International Standard provides guidance on mechanisms for ensuring that methods and processes used in the investigation of information security incidents are "fit for purpose". It encapsulates best practice on defining requirements, describing methods, and providing evidence that implementations of methods can be shown to satisfy requirements. It includes consideration of how vendor and third-party testing can be used to assist this assurance process.

This document aims to

— provide guidance on the capture and analysis of functional and non-functional requirements relating to an Information Security (IS) incident investigation,

— give guidance on the use of validation as a means of assuring suitability of processes involved in the investigation,

— provide guidance on assessing the levels of validation required and the evidence required from a validation exercise,

— give guidance on how external testing and documentation can be incorporated in the validation process.

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 27000:2013, *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 in ISO/IEC 27000:2013 and the following apply.

3.1
atomic
performing a single function only

Note 1 to entry: A *method* (3.11) for recovery of all live files from a device can be atomic if it relies solely on the use of filesystem meta-data. A method for recovery of all deleted files is unlikely to be atomic as it will require sub-methods which identify and extract particular file structures from the data on the storage device based on knowledge of file contents (e.g. .jpg, .png, .odt, XML, etc.).

3.2
black box testing
examining a process by using it to process known inputs and comparing the results against predicted outputs which reflect the requirements for the process

© ISO/IEC 2015 – All rights reserved

3.3
client
person or organisation on whose behalf the investigation is to be undertaken

[SOURCE: ISO/IEC 27042:2015, 3.2]

3.4
confirmation
formal assessment of existing objective evidence that a process is fit (or remains fit) for a specified purpose

3.5
contemporaneous notes
contemporaneous record
written record of actions taken and decisions made, produced at the same time or as soon afterwards as is practically possible, as the actions and decisions it records

Note 1 to entry: In many jurisdictions, it is necessary for contemporaneous notes to be handwritten in non-erasable ink in a tamper-evident notebook to assist with issues of authenticity and admissibility.

[SOURCE: ISO/IEC 27042:2015, 3.4]

3.6
examination
set of processes applied to identify and retrieve relevant potential digital evidence from one or more sources

[SOURCE: ISO/IEC 27042:2015, 3.7]

3.7
investigation
application of *examinations* (3.6), analyses, and interpretation to aid understanding of an incident

[SOURCE: ISO/IEC 27042:2015, 3.10]

3.8
investigative lead
person leading the investigation at a strategic level

[SOURCE: ISO/IEC 27042:2015, 3.11]

3.9
investigative team
all persons involved directly in the conduct of the investigation

[SOURCE: ISO/IEC 27042:2015, 3.12]

3.10
investigator
member of the *investigative team* (3.9), including the *investigative lead* (3.8)

[SOURCE: ISO/IEC 27042:2015, 3.13]

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* (3.11) should be *atomic* (3.1) (i.e. it should not perform more than one function) in order to enable re-use of methods and the *processes* (3.12) derived from them and to reduce the amount of work required to validate processes.

© ISO/IEC 2015 – All rights reserved

3.12
process
operational implementation of a *method* (3.11)

3.13
producer
creator or provider of a *tool* (3.17), including anyone who modifies or customises a tool

Note 1 to entry: The person(s) or organization(s) responsible for the creation or maintenance of a tool or customisation of a tool is the producer.

Note 2 to entry: Providing scripts to automate common functions modifies or customises a tool.

3.14
requirements
statement which translates or expresses a need and its associated constraints and conditions

Note 1 to entry: Requirements exist at different tiers and express the need in high-level form (e.g. software component requirement).

[SOURCE: ISO/IEC IEEE 29148:2011, 4.1.17]

3.15
requirements analysis
process (3.12) through which understanding and prioritisation of the *requirements* (3.14) is achieved

3.16
requirements capture
process (3.12) through which the *requirements* (3.14) for a process are discovered, reviewed, articulated, and documented

3.17
tool
software, hardware, or firmware used in a *process* (3.12)

3.18
validation
confirmation (3.4), through the provision of objective evidence, that the *requirements* (3.14) for a specific intended use or application have been fulfilled

Note 1 to entry: Validation is carried out on a *process* (3.12) to ensure that it is fit for purpose, i.e. to ensure that the process, as implemented, produces expected results in a consistent, repeatable, and reproducible manner.

[SOURCE: ISO/IEC 27004:2009, 3.17, Modified – Note 1 to entry has been added]

3.19
validation set
series of objective tests with clearly defined goals, inputs, and outputs, directly related to the agreed *requirements* (3.14) for the *process* (3.12) under *validation* (3.18)

3.20
verification
confirmation (3.4), through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: Verification only provides assurance that a product conforms to its specification.

[SOURCE: ISO/IEC 27004:2009, 3.18, Modified – Original note was removed, Note 1 to entry has been added]

© ISO/IEC 2015 – All rights reserved

3.21
verification function
function which is used to verify that two sets of data are identical

[SOURCE: ISO/IEC 27037:2012, 3.25, Modified – Notes were removed]

3.22
white box testing
testing which includes inspection of the implementation detail

3.23
work instruction
detailed description of how to perform and record a *process* (3.12)

[SOURCE: ISO/TR 10013:2001, 3.1, Modified - changed from plural to singular, task changed to process]

4 Symbols and abbreviated terms

ATA	AT Attachment
SATA	Serial ATA
USB	Universal Serial Bus

5 Method development and assurance

5.1 Overview

Assurance of suitability and adequacy of incident investigation methods can be required in order to demonstrate clearly that the investigator used methods which were fit for the purpose(s) of the investigation and used methods which were not subject to unacceptable errors or uncertainty. Digital evidence resulting from the application of unassured methods can be considered inherently flawed and subject to challenge which can result in it being rendered useless for the purposes of the investigation.

This standard presents an assurance model which includes all stages of development of the activities which make up an investigation, as described in ISO/IEC 27042:2015, from initial specification through to deployment and maintenance.

5.2 General principles

Assuring suitability and adequacy of incident investigation methods should follow a suitable model, such as the Plan-Do-Check-Act model used in ISO/IEC 9001:2000, in order to ensure that all processes are subject to review at least as often as they are used.

5.3 General development and deployment model

Prior to a process being deployed for use in investigations, it should undergo a proper development process in order to ensure that it is fit for purpose. Figure 2 shows typical stages in this process, which are:

— Requirements capture and analysis

— Process design

— Process implementation

— Process verification (optional and non-essential)

— Process validation

© ISO/IEC 2015 – All rights reserved

— Confirmation

— Deployment

— Review and maintenance

Each of these stages is discussed in more detail below.

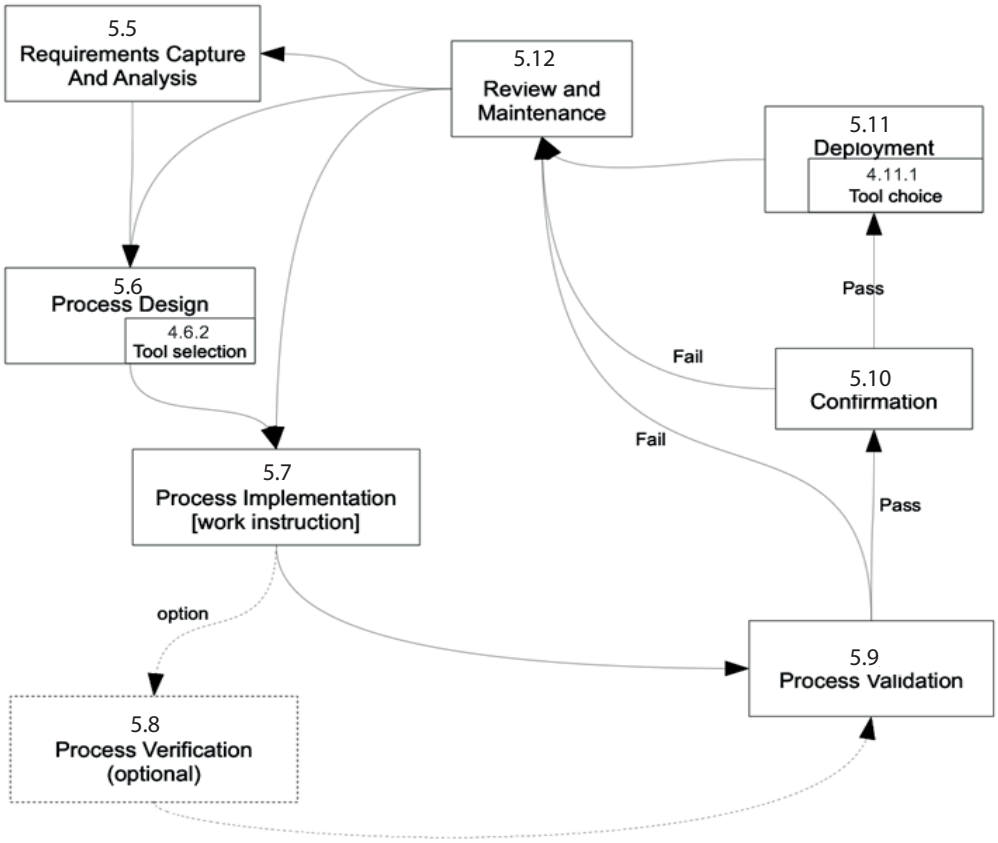

Figure 2 — Development and deployment process, including assurance stages

5.4 Assurance stages

Assurance should be included in the development model, above, in the following key assurance stages:

— Requirements capture and analysis

— Process validation

— Confirmation

— Review and maintenance

NOTE Further guidance on the conduct of these stages is given in the description of assurance models in Clause 5.

© ISO/IEC 2015 – All rights reserved

5.5 Requirements capture and analysis

5.5.1 General principles of requirements

Prior to designing a process for use in an examination, a proper set of requirements should be produced, accepted by the client and recorded in accordance with good practice. This set of requirements should be derived from the requirements identified for the complete investigation and may include both functional and non-functional requirements.

Each requirement defines an essential capability, characteristic or quality factor. Each individual requirement statement should be necessary, implementation-free (i.e. it states only what is required, not how the requirement should be met), unambiguous, complete, singular and consistent with the remainder of the requirements in the set.

Requirements vary in intent and in the kinds of properties they represent. They can be grouped together into similar types to aid in analysis and verification. Examples of types of requirements include:

— Functional – describe the functions or tasks to be performed and will include such considerations as expected inputs and outputs;

— Performance – defines the extent, how well, and under what conditions a function or task is to be performed;

— Interface – defines how the solution interacts with external systems, or how elements within the solution (including human elements) interact with each other;

— Process – include compliance with local laws and processes or administrative requirements;

— Non-functional – define how a solution is supposed to be, including quality requirements such as portability, reliability, maintainability and security, or human factors requirements such as safety, efficiency or health and wellbeing.

In addition to all essential requirements, the lists of requirements produced should also include clear definitions of the boundaries of operation associated with the anticipated potential digital evidence and related investigative processes (e.g. maximum file sizes, maximum and minimum number of input values).

A new list of requirements may need to be formulated for each investigation undertaken to ensure the examination correctly fulfils the specific case requirements. Using a monolithic approach to the design would require a significant validation overhead and so the user should where practically possible select predefined atomic stages which are compatible with dynamic user definable input parameters.

In that way the unique changes to the requirements will typically be limited to the specific case input parameters, and so the case specific validation would predominantly be limited to the specific parameters supplied to the case under investigation, and not the underlying function or process which should have been designed at the readiness phase.

EXAMPLE While specific keyword searches will be directly dependent on the case being investigated the keyword filter process should, if designed correctly, be an atomic process which is independent of the keywords used. The area which requires unique case specific validation be the definition of the correctness of the keyword[s] applied (i.e. the undefined uncertainty error will be in the user's design of the specific search terms used, for instance only searching for "Joe Blogs" would miss references to "Joe Bloggs", "Mr Blogs", "J. Blogs", "Joe", "Joey", etc.).

The incident under investigation should be clearly identified and defined, including limitations to the scope of the investigation. Sources of potential digital evidence and questions to be answered should be identified. Sources of risk and their potential effects on the investigation, personnel and systems should also be identified.

 © ISO/IEC 2015 – All rights reserved

Once the requirements for the investigation have been identified, the investigative team should then develop requirements for the examinations, analyses and processes which will make up the investigation (see ISO/IEC 27042:2015).

5.5.2 Functional Requirements

Functional requirements are those stemming directly from investigative needs and which are expected by the users of the process. They do not define how the process should operate but will include such considerations as expected inputs and outputs. All functional requirements should be satisfied by the investigation.

EXAMPLE The need to process a particular type of filesystem is a functional requirement as it is derived directly from a source of potential digital evidence.

5.5.3 Verification of requirements

Undertaking an exercise to verify the requirements will ensure that the specified requirements are well formed and that the needs of the investigative method have been adequately expressed. It involves an analysis of the recorded requirements to identify problems such as conflicting, missing, incomplete, ambiguous, inconsistent or incongruous requirements. Any identified problems should be resolved before moving on to subsequent assurance stages.

5.6 Process Design

5.6.1 Overview

The design of a process should take account of all requirements identified as a result of the requirement capture and analysis stages. It should give detail of how the method will be implemented, taking account of accepted non-functional requirements and is the point at which tool selection should be carried out. Design need not specify the exact detail of each element of the process, but should clearly identify the flow of activity and evidential material from one step to the next.

5.6.2 Tool Selection

During the design phase, any tools which may participate in the process should be identified and their role(s) in the resulting process identified. Where several tools can perform the same function in the process, it may be useful to identify some or all of these tools in order to cope with variation in operating environments (e.g. write blockers may offer different interfaces such as ATA, SATA, USB etc.) Care should be taken, however, to ensure that allowing for variable requirements in this way does not adversely affect the atomic nature of the process.

The documented process should define the group of tools which should be considered for use, along with the identified and, where possible, quantified risk to specific atomic functions of each of the tools listed.

5.6.3 Uncertainty and risk evaluation

All tools, be they hardware or software based, will be prone to a level of error. This is an unavoidable reality which is caused by the fact that they are physically[8)] manufactured components, designed and implemented to within a predefined tolerance of an ideal which can never be guaranteed to be 100 % perfect. The error may range from relatively high to insignificantly minute, but either way it will exist and can never be completely eliminated, only controlled and accounted for.

The investigator's familiarity with the proposed tool or process should also be taken into account, as the less familiar a user is with a tool or process, the greater the chance that additional uncontrolled errors will occur. Effective training and routine proficiency testing are widely accepted techniques for helping to minimize this specific type of error.

8) Software resides on a physical computer and so is affected by both hardware and software based errors.

© ISO/IEC 2015 – All rights reserved

These errors are collectively known as the uncertainty characteristics of each element or component of a process, and can be, in simple terms, characterized as the strengths or weaknesses of the process.

The uncertainty characteristics will typically be additive in nature in a linear system, such as the model described, and so will normally increase proportionally in line with the number of processes used.

To compensate, robust proportional overlapping processes should be designed to ensure they strengthen the provenance of all the digital evidence found.

Before using a preferred tool or method to conduct an investigation the investigators should consider the likely effects of all the weaknesses of the complete process sequence selected. A formal understanding of the weaknesses of a process enables these errors to be effectively controlled through the use of correct process selection and robust documented risk analysis or assessments.

The use of validated atomic elements within a process sequence can also be a significant aid in helping to simplify the understanding and controlling these uncertainties, and is the primary reason why it is central to assurance methods detailed in this document.

Finally, it should also be understood that even though a specific process may exhibit unknown or high weakness it does not necessarily exclude it from consideration as appropriate. Indeed in some cases, where it is the only process available to complete a required task it will likely be considered invaluable.

5.7 Process Implementation

5.7.1 Overview

Once the design has been completed, it should be implemented in the form of a documented detailed work instruction which gives step by step instructions for the correct operation of each step of the process. During this stage, final decisions about tool selection (e.g. choosing between alternative versions of the same tool type) may be taken in order to improve the process.

5.7.2 Tool choice — guidance for deployment

Where the design of the process includes a list of tools which may be used to perform the same, or similar, functions, the work instruction should provide guidance (see also 5.6.2) on how the investigator should choose the appropriate tool for the conditions encountered during the examination. Care should be taken, however, to ensure that allowing for variation, in this way, does not adversely affect the atomic nature of the process.

Maintenance of a risk register, which includes assessments of risk and uncertainty for available tools, can assist with tool choice. A tool can start with a blank entry in this register, but this should be considered as a risk as it is likely to indicate that the tool is new and has not yet been evaluated in any detail.

A tool which is not the most suitable for the particular circumstance might still be chosen for use as long as its evaluation and defined process usage is clearly defined along with its associated risks.

NOTE A tool may be chosen because it is the best available from a set of generally poor solutions, or because it is the only tool available which can produce any form of usable result.

5.8 Process Verification

5.8.1 General principles of verification

Verification provides a level of assurance that a process or tool conforms to its specification. This does not guarantee that it will operate in the desired way in the context of a complete investigation or process. Evidence of verification against requirements which are similar to those for the intended use should be treated as an initial indicator that the tool or process may be suitable for deployment in the context of an investigation, but not a complete assurance that it will satisfy the requirements for the intended use. Verification should be considered an optional, but potentially useful, part of assurance.

© ISO/IEC 2015 – All rights reserved

5.8.2 Verification of processes

Following development of the work instruction it should be compared with the design and evidence produced, to show how the work instruction complies with the design. The design may be amended to reflect implementational changes made during production of the work instruction (e.g. a result of unexpected or new tool behaviours). Verification will usually be carried out using "white box testing" in order to allow comparison with the design.

5.8.3 Verification of tools

Tools can be verified by the user, the producer, or a third party. Where a tool is verified by the producer or a third party, the verification will normally be based on the design requirements for the tool. A third party or producer verification is only useful, as part of the validation, if complete information about the verification is provided, including the design requirements against which the tool was verified. If these design requirements can be mapped onto the requirements for the tool's participation in the process under consideration, the matching verification data can provide partial evidence of validation for those stages of the process in which the tool participates. Verification is not sufficient, in its own right, to achieve validation of a process as verification does not consider the way in which the user of the tool intends to use the tool in the process.

5.9 Process Validation

5.9.1 General principles of validation

Validation demonstrates that the process defined in the work instruction fulfils the requirements agreed with the client. It does not directly consider the implementation defined by the work instruction, but provides evidence that the process produces correct outputs for the defined set of inputs. Where possible, the validation process should also determine boundary conditions and error rates. Typically, the validation process will be conducted through "black box testing" to ensure that knowledge of implementational detail does not affect the conduct of the testing or influence the results.

A validation plan and associated data should be produced independently of the design and implementation phases and should be based solely on the agreed requirements.

NOTE Processes which use unverified tools or methods can be validated if they provide consistent results (cf. requirement for repeatability and reproducibility described in ISO/IEC 27037:2012).

5.9.2 Comprehensive validation

Comprehensive validation refers to a validation which tests a process under all possible conditions (e.g. on all possible hardware configurations for all possible inputs). This is not considered essential and is likely to be prohibitively expensive in terms of time and resources required. Where a process forms a key part of several analyses, and is likely to be deployed regularly, comprehensive validation can be essential, but this may only apply to processes which are used in multiple different types of investigation by multiple different investigative teams.

In other circumstances, (e.g. for a "one-off" process intended to solve an immediate problem but not likely to be re-used), a sufficient validation may be adequate. Post-deployment validation should be avoided unless absolutely necessary. Some simple pre-deployment validation should always be attempted (based on a limited set of requirements) but more thorough post-deployment validation should be applied as soon as practically possible, especially if the process is to be used in the future.

EXAMPLE A process for recovering data from magnetic stripe cards may be comprehensively validated as there are relatively few formats for storing data on such cards.

5.9.3 Sufficient validation

Sufficient validation refers to validation against agreed functional and non-functional requirements for the conditions pertaining at the time of the investigation. It is not necessary to validate a method

© ISO/IEC 2015 – All rights reserved

against software and hardware configurations which will not be relevant in the investigation, nor is it necessary to consider validation for data which will not be processed.

A sufficient validation is one which shows that the process produces correct results for the type of inputs encountered in the investigation under consideration, i.e. a sufficient validation shows that a process is fit for a particular intended use as defined by the identified requirements.

5.9.4 Fully validated processes

A process which has passed validation may be described as fully validated for the intended use defined in the validation plan. A process should, normally, not be employed until it has been fully validated.

5.9.5 Failed validation

If a process does not pass validation, the requirements, design and implementation should be reviewed and amended appropriately. Once this is complete, the process should be subjected to validation again.

5.10 Confirmation

The final step before deployment of the process is confirmation. This formally assesses whether the process meets the agreed requirements and provides formal evidence that the process is fit for use in the investigation.

For confirmation to be carried out the evidence of validation for the process should be checked against the agreed requirements for the intended use of the process. A process may only be confirmed if it is fully validated.

A process which has previously been validated may be confirmed without further validation if it is fully validated for the current investigation. This includes processes which have been subject to external validation.

Confirmation can be the final step of a validation or re-validation, or can constitute a step, in its own right, which provides a formal record that previously produced validation evidence, from a prior investigation, is adequate for the current investigation.

5.11 Deployment

Once the process has been accepted it can be deployed for use in the examinations which make up the investigation. Any and all deviations from expected results or behaviours should be recorded and remedial actions taken. Where remedial actions involve a change to the process or the deviation from expected behaviour conflicts with previous validation results, revalidation may be required.

5.11.1 Tool choice

During deployment of a process, the investigator may have to choose amongst several tools which provide the same, or similar, functionality. Although the work instruction should contain guidance on how this choice should be made, the investigator should also maintain a contemporaneous record of the tool choices made and the factors which influenced these choices.

5.12 Review and Maintenance

Following deployment of a process, its performance should be reviewed to identify any missing requirements, or changes which may be required to cope with changes to tools used (e.g. forced upgrades due to changes in platforms, end of life conditions etc.). Following review, it may be necessary to revert to the Requirements Capture and Analysis, Process Design or Process Implementation phases to produce a maintenance action. Whichever phase is used, it and its successors should be completed to ensure that the validation of the revised process can be confirmed.

© ISO/IEC 2015 – All rights reserved

6 Assurance Models

6.1 Overview

In the context of the assurance stages, individual assurance stages should be, as far as practically possible, carried out independently of the development of the processes (i.e. carried out by someone other than the developers), in order to provide an additional level of confidence that processes are truly adequate for their intended use. In order to achieve this, steps should be taken to ensure that assurance stages are carried out in a manner which ensures that they are not unduly influenced by design and implementation considerations.

This section discusses assurance models which can be used to assist in ensuring that undue influence is not introduced. In general, assurance may be carried out within the organization which will use the processes (see 6.2), by another organization (see 6.3) or using a combination of the two mechanisms (see 6.4). Whichever model is used, proper evidence of assurance (see Clause 7) should be produced and maintained.

6.2 In-house assurance

In-house assurance may be applied to any investigative processes which are to be deployed within the organization. The organization should use a validation set which represents its own intended uses for the processes, carry out the relevant tests and record that the processes are fit for purpose through formal confirmation.

6.3 External assurance

In this assurance model, responsibility for conduct of the validation is passed to another body.

Where the external body is conducting validation only, the implementing organization and validating body should agree the requirements and validation set prior to conduct of the validation and reviewed as part of the confirmation phase.

Where the external body has produced the processes, the implementing organization should take care to ensure that a sufficient validation, based on the confirmation requirements, is produced in order to meet the confirmation criteria for the processes. Detail of the requirements and validation set should be obtained from the validating body.

6.4 Mixed assurance

In the mixed assurance model, a combination of the two modes described above ("in-house" and "external") is used. This will typically happen where an externally produced process is to be implemented and deployed with some modification to requirements in order to meet local requirements. The external validation results may need to be complemented by additional in-house validation in order to provide evidence that the process meets the modified requirements.

EXAMPLE A published validated process for the imaging of magnetic discs could be adapted for the imaging of solid-state storage devices. If no adequate external validation evidence is available, the modified process should be subjected to additional in-house validation.

7 Production of evidence for assurance

7.1 Overview

Digital evidence can be challenged on the grounds that methods used to produce it were not fit for purpose. For this reason it is important that evidence of fitness for purpose can be produced. This can be achieved by applying the assurance stages, described in Clause 5, and maintaining thorough records of the assurance process. A method for producing this evidence of assurance is described below.

© ISO/IEC 2015 – All rights reserved

7.2 Pre-validation preparation

Prior to validation being conducted a validation plan and associated validation samples (the plan and samples together constitute the validation set) should be produced. In order to avoid possible conflict caused by knowledge of implementation and assumptions made, the validation set should be carried out by a party not involved in the design, implementation and verification of the process. If this is not possible, the process used for validation should be clearly and consistently documented so that it may be reviewed by an independent party to assess impartiality.

The validation plan will normally define a series of black-box tests, mapped directly to agreed requirements. Each test will state the inputs to be presented and the expected outputs. Tests should actively aim to stress-test processes, including tools which can participate in those processes, to ensure that they are sufficiently robust and fit for purpose.

The validation set should normally be subjected to a final check to ensure that it is sufficient and appropriate to satisfy the stated requirements. This is particularly important where third-party validation sets are to be used. Where a clear statement that the validation set is consistent with the agreed requirements is not produced, the validation may be considered incomplete and the processes to which it is applied may be declared unvalidated as a result. This check should not be carried out solely by the third-party but should be overseen by the organization which will be responsible for dealing with the results of any investigation.

7.3 Producing Evidence of Validation

Once the validation set has been confirmed, the process should be carried out, according to the work instruction, for each test defined in the validation set, using the corresponding validation samples. A record should be kept of the outcome of each test (i.e. pass or fail) with details of any problems encountered or changes required as a result of the validation process. This record should include detail of the validation set used and forms the evidence of validation.

7.4 Maintenance of Validation

Validation sets and evidence of validation should be subject to periodic review to ensure that they are still appropriate for the intended uses of the associated processes. Processes should be audited to ensure that their evidence of validation is still correct and that they remain appropriately validated.

A process which is no longer appropriately validated or no longer has current evidence of validation (e.g. because the review date has passed or because of changes in non-functional requirements) should be considered unvalidated until re-validation occurs.

If a validation set is amended/updated (e.g. due to changes in functional or non-functional requirements) all processes validated using the set should be checked to determine if the revised validation set applies to them. If the revised validation set is not applicable, processes can remain validated through the use of the original validation set. If the revised validation set is applicable to existing processes, they should be re-validated using the revised validation set.

7.5 Validation of Examinations

An examination may be considered validated if all the processes making up the examination are validated. It may be necessary to carry out a separate validation of an examination for added assurance of suitability and adequacy, particularly where examination-specific linking processes (e.g. carrying out minor transformations on the output from a process or analysis to make it suitable for input to another) have been introduced. Care should be taken to ensure that the validation of an examination is as complete as possible.

Proficiency testing (See ISO/IEC 17043:2010) may be used to provide an additional degree of assurance of suitability and adequacy of examinations, but should not be used as a substitute for proper assurance as proficiency tests usually only test the application of processes in limited test conditions.

© ISO/IEC 2015 – All rights reserved

7.6 Validation of Investigations

An investigation which contains only validated examinations can be considered to be validated.

Investigations are likely to include stages where the outputs of processes and examinations require interpretation and this may be dependent on the competence of the investigator. Therefore, an investigation should be considered fit for purpose where the examinations and processes resulting in factual information have been fully validated.

Evidence of competence of staff and proficiency testing will provide an additional level of assurance that an investigation is fit for purpose.

© ISO/IEC 2015 – All rights reserved

Annex A
(informative)

Examples

A.1 Work instruction

Process/activity	001: Imaging of SATA hard disk
Purpose	Produce evidential copy of hard disk
Report to	Digital Evidence Analyst
Legislation and Policies	Evidence handling policy, local legislation, ISO/IEC 27035, ISO/IEC 27037, ISO/IEC 27042, ISO/IEC 27041
Equipment required	SATA interface adapter, SATA power supply, SATA write blocker (hardware or software), imaging tool (software + associated workstation or hardware imaging device), "sterile" storage device large enough to accept image in chosen format.
Staff competence	Compatible with UK e-crime NOS CO.3 "Capture and Preserve Potential Electronic Evidence" or ISO/IEC 27037:2012 example competence definition
Proficiency	trained or experienced in use of equipment selected and this process.
Process	Check seals and establish continuity. Remove source device from packaging.
	Record device ID and properties as declared on labels
	Ensure write blocking is active and connect device to appropriate interface. Record actions.
	Record device ID and properties as determined by tools
	Verify that target storage has sufficient capacity
	Use verification function (see ISO/IEC 27037:2012) to establish "signature" for original device. Record results.
	Carry out imaging using appropriate tool and check for errors during the process. Record actions and results.
	At end of process, use verification function to establish "signature" for image and ensure that it matches the original device, or account for differences (e.g. because of errors). Record actions and results.
	If errors present, determine if error is in original device or image and follow process for that situation.
	If no errors found, safely disconnect original device and repackage, following correct continuity procedure. Record actions.
	If no errors found, safely disconnect target device and package appropriately for future examination. Record actions.
	Return source device to evidence store. Record actions.
	Submit target device to evidence store. Record actions.

© ISO/IEC 2015 – All rights reserved

A.2 Validation plan

Process (Work Instruction) to be validated	001: Imaging of SATA hard disk
Validation method	1) Fully functioning drives a) Select representative sample of most commonly encountered drives types by manufacturer and capacity from pool of known good drives. b) prepare drives by writing known data to each one (e.g. complete wipe of drive using "dd" to write zeroes, followed by partitioning and installation of operating system). b) Apply work instruction to produce a copy of each drive. c) Apply verification function to test drive and copy to check that images are correct. d) Apply validated preview work instruction to source and copy to check that contents are equivalent. 2) Damaged drives a) Select representative sample of most commonly encountered drive types, by manufacturer and capacity, from known bad pool. b) Use validated diagnostic work instruction to locate and record areas of damage on drive. c) Use validated preview work instruction to record contents of each drive. d) Apply Imaging work instruction to produce a copy of each drive in turn e) Apply validated preview work instruction to obtain and record contents of each copy. f) Compare contents of copy against contents of original drive, ensuring that damaged areas have been handled appropriately (i.e. each damaged block on the source drive should result in a null block in the copy)
Validation success criteria	1) For fully functioning drives, the copy should produce the same result from the verification function as the original drive. The contents of the source drive and copy should be identical when the preview work instruction is applied. 2) For damaged drives, all readable data on the source drive should appear in the equivalent location in the copy. The contents of the source drive and copy should be equivalent when the preview work instruction is applied.
Version: 001	**Created:** 12/Apr/2012
Last checked: 11/Apr/2013	**Review due:** 12/Apr/2014

© ISO/IEC 2015 – All rights reserved

A.3 Evidence of validation

Reference number	V001	Date	13/Apr/2013
Work instruction under validation		001: Imaging of SATA hard drive	
Validation method / version		001: Imaging of SATA hard drive version / 001	
Test	Test description	Result	Outcome
1	Method 1 applied to WD5000AJS (Caviar SE) s/n WCAPW0863110. Drive wiped and Windows 7 installed on single partition.	Drive MD5: 853f9d81e22a4e-03f92aa61171471516 Copy MD5: 853f9d81e22a4e-03f92aa61171471516 Previews: Directory hierarchies identical, 100 dip-sampled files identical.	Pass
.	.	.	.
.	.	.	.
.	.	.	.
99	Method 2 applied to WD5000 AJS (Caviar SE) s/n WCAPW0862110. Known to have bad sectors at 64, 1035, 9119,9120,9121,9122	WD diagnostic confirmed bad blocks as listed. Imaging process reported bad blocks as listed. Previews: Directory hierarchies identical. 99 dip-sampled files identical. One dip-sampled file used sector 9120 and was not identical. Sectors in copy corresponding to damaged sectors contained nulls.	Pass
Version: 001		**Created:** 12/Apr/2012	
Last checked: 11/Apr/2013		**Review due:** 12/Apr/2014	

© ISO/IEC 2015 – All rights reserved

A.4 Confirmation statement

Investigation Reference	INT/001
Requirements	Determine if hard drives in standard workstations contain spreadsheet data Produce evidence copies of filesystems with spreadsheet data Recover spreadsheet data from evidence copies of filesystems
Processes / Work Instructions to be deployed	Validation evidence and Date
001: Imaging SATA hard drives 002: Triage of SATA hard drives with NTFS filesystems 003: Recovery of spreadsheet data from NTFS filesystems	V001: 13/Apr/2013 V002: 01/Dec/2012 V006: 12/Nov/2012
Confirmation statement	The requirements of the processes match those of the investigation. The processes have been subjected to sufficient testing to provide sufficient evidence of validation. I therefore confirm that the processes, listed above, are suitable for deployment in this investigation.
Name	E. Lestrade
Signature	
Date	14/Apr/2013

© ISO/IEC 2015 – All rights reserved

Bibliography

[1] ISO/IEC 17024:2012, *Conformity assessment — General requirements for bodies operating certification of persons*

[2] ISO/IEC 17043:2010, *Conformity assessment — General requirements for proficiency testing*

[3] ISO/IEC/IEEE 29148:2011, *Systems and software engineering — Life cycle processes — Requirements engineering*

[4] ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories*

[5] ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management — Measurement*

© ISO/IEC 2015 – All rights reserved

ICS 35.040

Price based on 18 pages

© ISO/IEC 2015 – All rights reserved