INTERNATIONAL STANDARD

ISO/IEC 27043

First edition
2015-03-01

Information technology — Security techniques — Incident investigation principles and processes

Technologies de l'information — Techniques de sécurité — Principes d'investigation numérique et les processus

Reference number
ISO/IEC 27043:2015(E)

COPYRIGHT PROTECTED DOCUMENT

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

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*.

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

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

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

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.

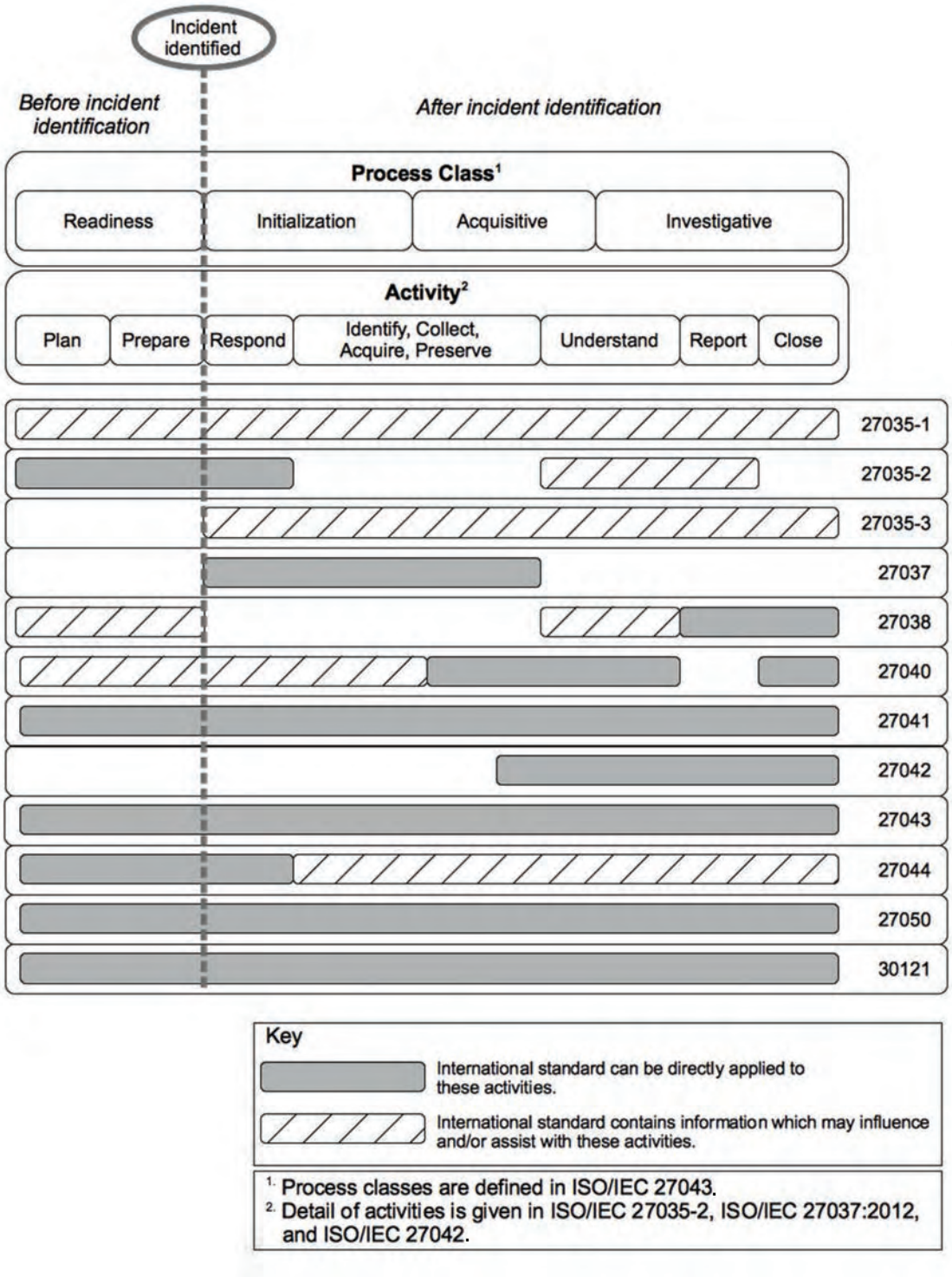

Figure 1 — Applicability of standards to investigation process classes and activities

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]

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]

3.12
potential digital evidence
information or data, stored or transmitted in binary form, which has not yet been determined, through the process of examination and analysis, to be relevant to the investigation

[SOURCE: ISO/IEC 27042:—, 3.15, modified — Definition adapted to refer to the abstract process "examination and analysis" rather than analysis only; note 1 and note 2 to entry not included.]

3.13
preservation
process to maintain and safeguard the integrity and/or original condition of the potential digital evidence and digital evidence

[SOURCE: ISO/IEC 27037:2012, 3.15, modified — Added "and digital evidence".]

3.14
process
set of activities that have a common goal and last for a limited period of time

Note 1 to entry: Also see ISO/IEC 27000 and ISO 9000 for similar definitions of a process.

Note 2 to entry: The meaning of "process" in this International Standard refers to a higher level of abstraction than the definition of "process" in ISO/IEC 27041.

3.15
readiness
process of being prepared for a digital investigation before an incident has occurred

3.16
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[SOURCE: ISO/IEC 27004:2009, 3.17]

3.17
verification
confirmation, 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 27041:—, 3.20]

3.18
volatile data
caused by data that is especially prone to change and can be easily modified

Note 1 to entry: Change can be switching off the power or passing through a magnetic field. Volatile data also includes data that changes as the system state changes. Examples include data stored in RAM and dynamic IP addresses.

[SOURCE: ISO/IEC 27037:2012, 3.26, modified — Inserted "caused by" at the beginning of the original definition.]

4 Symbols and abbreviated terms

DVR	digital video recorder
IP	Internet Protocol
JPEG	Joint Photographic Experts Group

RAM random access memory

PKI public key infrastructure

5 Digital investigations

5.1 General principles

Digital investigations are in practice applied whenever it is needed to investigate digital evidence as a result of an incident, whether an incident is of criminal nature or not. There are many kinds of digital investigations, such as on desktop computers, laptops, servers, data repositories, handheld/mobile device investigations, investigations on live data (e.g. network and volatile data investigations), and investigations on digital appliances such as DVRs, game consoles, and control systems. The digital investigation process, however, is formulated in such a way that it is applicable to any kind of digital investigation.

5.2 Legal principles

An overview is given of the legal requirements pertaining to digital investigations and especially the admissibility of digital evidence in a court of law. It should be noted that legal requirements may differ extensively in different jurisdictions across the world. The premise is not to advocate specific legal systems, but rather to note the generic requirements in terms of legal issues that can be adopted by the legal system of a specific jurisdiction. Depending on the particular laws in a particular jurisdiction, specific consideration and care should be taken when an accused is found to be innocent in a court of law. For example, due diligence and care should be taken to ensure

— safe deletion (see ISO/IEC 27040) of the evidence and case data at the end of the court case if so required,

— secure preservation of the media and devices holding the potential digital evidence as far as possible, secure preservation of the digital evidence itself and secure preservation of the investigation results for possible future reference, and

— notification to the subject of the investigation results.

In some jurisdictions it is acceptable that if scientific, technical, or other specialized knowledge will assist the court to understand the evidence or to determine a fact in issue, a witness accepted as an expert by virtue of their experience, knowledge, skill, training, or education, may testify thereto in the form of an opinion.[2] To help assure admissibility of expert opinion, the following factors should be considered (as applicable in the particular jurisdiction):

— whether the theories and techniques employed by the scientific expert have been tested;

— whether they have been subjected to peer review and publication;

— if an error rate for the technique is known it should be reported;

— whether they are subject to standards governing their application;

— whether the theories and techniques employed by the expert enjoy widespread acceptance.

NOTE The admissibility of the evidence itself and the admissibility of expert opinion about the interpretation of the evidence are two different issues to consider. For example, a technical witness may be able to testify about how evidence was acquired, preserved, etc., to address the adequacy of those processes without the necessity of qualifying as an expert. In other words, the expert may also testify to technical facts. Also see ISO/IEC 27042:—, 8.2.

Requirements for admissibility may vary considerably between jurisdictions and for that reason it is highly advisable to obtain competent legal advice regarding those specific requirements. However, many jurisdictions will include at least the following in their admissibility requirements for evidence:

— relevance — the evidence should have some relevance to the facts in dispute.

— authenticity — the evidence should be shown to be what it purports to be. For example, if a particular JPEG image extracted from the hard drive of a particular server is relevant to a question of fact under dispute, the trier of fact will demand demonstrable assurance that the drive is in fact from that particular server, that it has not been modified in any way since its collection, that the process used to extract the JPEG image is trustworthy, etc.

It is important that legal issues need to be applied throughout the entire investigation process. For each and every sub-process, a legal check should be conducted in order to determine whether the legal laws and regulations are adhered to within the particular jurisdiction. It is recommended to seek legal advice within the particular jurisdiction in case of uncertainty.

6 Digital investigation processes

6.1 General overview of the processes

The digital investigation processes described in this International Standard are purposely designed at an abstract level so that they can be used for different digital investigations and different types of digital evidence. The use of this methodology is intended to aid the design and development of high-level processes with the intent to subsequently decompose them into atomic processes (see ISO/IEC 27041). Also, the processes aim to be comprehensive in that they represent a harmonization of all published digital processes by the time of writing this International Standard. The investigation processes are organized in a succinct fashion and describe how to follow these processes.

6.2 Classes of digital investigation processes

The digital investigation processes constitute a long list. In order to abstract digital investigation processes at a higher level, they can be categorized into the following digital investigation process classes:

— readiness processes: That class of processes dealing with pre-incident investigation processes. This class deals with defining strategies which can be employed to ensure systems are in place, and that the staff involved in the investigative process are proficiently trained prior to dealing with an incident occurring. The readiness processes are optional to the rest of the digital investigation processes. The reason for this is explained in more detail in 7.1. Readiness processes include the following:

  — scenario definition;

  — identification of potential digital evidence sources;

  — planning pre-incident gathering;

  — storage and handling of data representing potential digital evidence;

  — planning pre-incident analysis of data representing potential digital evidence;

  — planning incident detection;

  — defining system architecture;

  — implementing system architecture;

  — implementing pre-incident gathering, storage, and handling of data representing potential digital evidence;

  — implementing pre-incident analysis of data representing potential digital evidence;

  — implementing incident detection;

  — assessment of implementation;

  - implementation of assessment results.

- initialization processes: That class of processes dealing with the initial commencement of the digital investigation. Initialization processes include the following:
  - incident detection;
  - first response;
  - planning;
  - preparation.
- acquisitive processes: That class of processes dealing with the physical investigation of a case where potential digital evidence is identified and handled. Acquisitive processes include the following:
  - potential digital evidence identification;
  - potential digital evidence acquisition;
  - potential digital evidence transportation;
  - potential digital evidence storage.
- investigative processes: That class of processes dealing with uncovering the potential digital evidence. Investigative processes include the following:
  - potential digital evidence examination and analysis;
  - digital evidence interpretation;
  - reporting;
  - presentation;
  - investigation closure.
- concurrent processes: That class of processes that continues concurrently alongside the other processes. This class of processes differ from the previous classes in the sense that they happen in tandem with the other processes instead of linear. In addition, the particular order in which the concurrent processes execute is irrelevant as opposed to the other non-concurrent processes. Concurrent processes include the following:
  - obtaining authorization;
  - documentation;
  - managing information flow;
  - preserving chain of custody;
  - preserving digital evidence;
  - interaction with the physical investigation.

Figure 2 shows the relationships between the various classes of digital investigation processes.

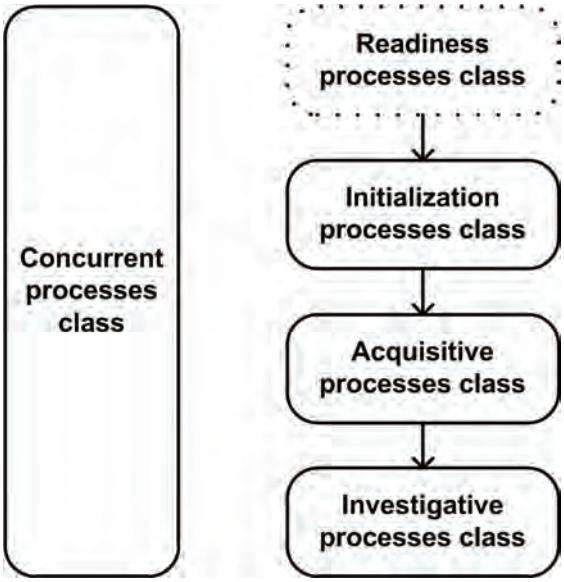

Figure 2 — The various classes of digital investigation processes

NOTE The dotted lines around processes in all figures indicate that the particular process is optional.

The six concurrent processes are aimed at allowing the said processes to be executed as on-going processes. The reason for having the concurrent processes is mainly to assure admissibility of digital evidence into a legal system, since, in the case of not having such processes, any investigation may run the risk that the admitted potential evidence might not be suitable for litigation due to improper handling, and documentation of potential digital evidence. These concurrent processes are, thus, based on principles that need to be followed throughout a digital investigation, alongside with the other classes of processes.

The digital investigation processes are multi-tiered, where each process would contain a set of sub-processes. Sub-processes can only be fully defined for a specific type of incident and investigation. Legal rules will also likely have a high impact on the definition of sub-processes. These various classes of digital investigation processes are described in more detail in the clauses to follow, i.e. Clauses 7 to 11.

7 Readiness processes

7.1 Overview of the readiness processes

Readiness processes include that class of processes dealing with setting up an organization in such a way that, in the case that a digital investigation is required, such organization possesses the ability to maximize its potential to use digital evidence whilst minimizing the time and costs of an investigation. This class of processes is optional to the digital investigation processes since it is the prerogative of the organization to implement it rather than the task of the investigator(s).

There are four aims for having digital investigation readiness processes in organizations:

a) to maximize the potential use of digital evidence;

b) to minimize the costs of digital investigations incurred either directly onto the organization's system, or related to the system's services;

c) to minimize interference with and prevent interruption of the organization's business processes;

d) to preserve or improve the current level of information security of systems within the organization.

Figure 3 depicts the readiness processes groups as described above, grouped in process groups as follows: *planning processes group, implementation processes group,* and the *assessment processes group*. The *planning processes group* includes readiness processes, as depicted in Figure 4, that are concerned with planning activities, including the

— scenario definition process,

— identification of potential digital evidence sources process,

— planning pre-incident gathering process,

— storage and handling of data representing potential digital evidence process,

— planning pre-incident analysis of data representing potential digital evidence process,

— planning incident detection process, and

— defining system architecture process.

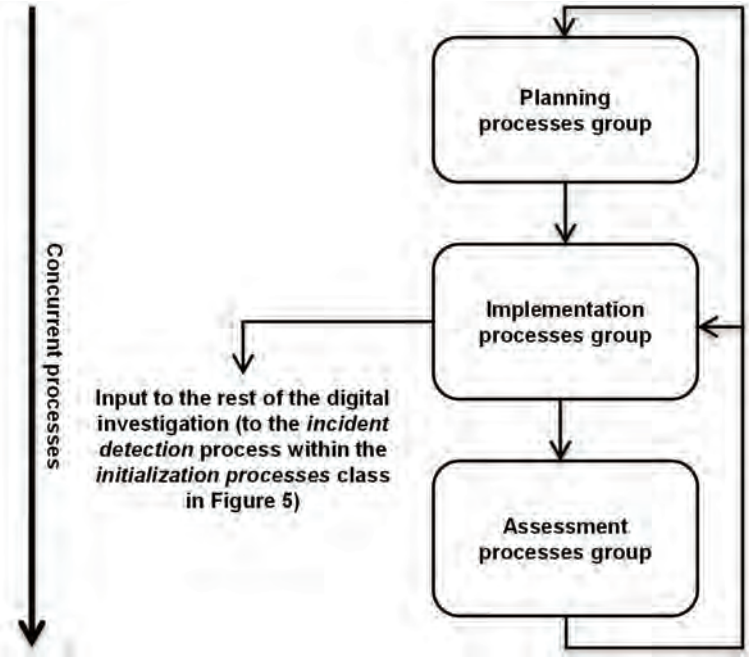

Figure 3 — Readiness processes groups

The *implementation processes group* includes readiness processes, as depicted in Figure 4, that are concerned with implementing the planned activities in the planning processes group, including the

— implementing system architecture process,

— implementing pre-incident gathering, storage, and handling of data representing potential digital evidence process,

— implementing pre-incident analysis of data representing potential digital evidence process, and

— implementing incident detection process.

The *assessment processes group* includes readiness processes, as depicted in Figure 4, that are concerned with the assessment of the implementation success from the implementation process group, including the

— assessment of implementation process, and

— implementation of assessment results process.

Note that the *implementing incident detection* process links to the *incident detection* process as shown in Figure 8 in order to establish the link from the readiness processes group to the initialisation processes group.

Input to all processes in Figure 4 includes all information regarding system architecture, technology (hardware and software), policies, procedures, and business processes of an organization where applicable. The input should also consider the four aims for the readiness processes as mentioned earlier. The input arising from the mentioned four aims are referred to as pre-known system inputs in the remainder of this International Standard.

The readiness processes are iterative, which implies that, after the last process, one can return to previous readiness processes, as shown in Figure 4. For example, when, during the *assessment of implementation* process, one notes that certain defined system architecture has not been properly implemented, one would need to go back to the *implementing system architecture* process. Another example is if one notes that plans made during the *planning pre-incident gathering, storage and handling of data representing potential digital evidence* process are not in line with aims for having digital investigation readiness processes in the particular organization, one could go back to the *planning pre-incident gathering, storage, and handling of data representing potential digital evidence* process in order to change those plans accordingly.

Each of the readiness processes are explained in the clauses that follow.

7.2 Scenario definition process

In this process, one should examine all probable scenarios where digital evidence might be required. The output of this process includes the defined scenarios.

It is also recommended that a proper risk assessment is performed during this process for each identified scenario respectively. A risk assessment would enable one to better identify possible threats, vulnerabilities and related scenarios that would expose particular information assets. Based on the assessed risk from certain threats, vulnerabilities or scenarios, one can, in later processes, better decide on the required controls to achieve investigation readiness within an organization. This will enable an organization to take into account the risk level, costs, and benefits of possible controls in a bid to reduce the identified risk.

7.3 Identification of potential digital evidence sources process

In this process, one should identify potential sources of digital evidence within an organization. The output of this process is the defined potential sources of digital evidence.

Some of the identified potential sources might not be available. For example, if access logs are not introduced within the system, it means that access logs will not be available as a source of data in the case of a digital investigation. In that case, controls should be explored to make the identified source available.

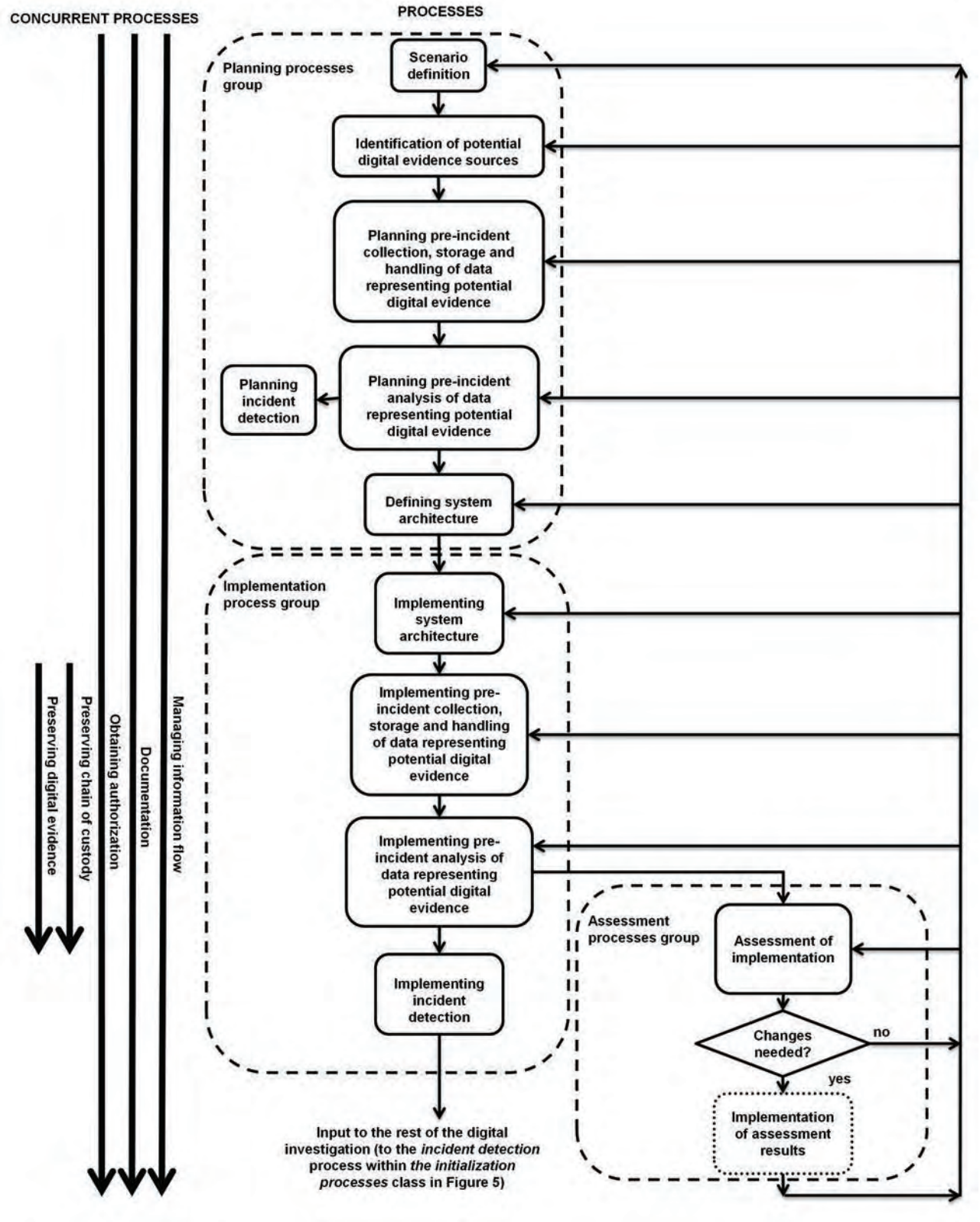

Figure 4 — Readiness processes

7.4 Planning pre-incident gathering, storage, and handling of data representing potential digital evidence process

In this process, one should define activities for pre-incident gathering, storage and handling of data representing potential digital evidence. The output of this process includes the defined activities for pre-incident gathering, storage, and handling of data representing potential digital evidence.

The gathering period of certain types of data, is to be determined based on a risk assessment. The gathering, storage, and handling of data also have to conform to digital investigation principles in order for digital evidence to be admissible in a court of law. Lastly, the retention period of data is to be determined based on following factors:

— risk assessment;

— previous experience regarding incident detection, data quantities, network capacity, and all other matters that could influence cost or efficiency of this process;

— laws within the particular jurisdiction;

— regulations;

— business-specific requirements.

7.5 Planning pre-incident analysis of data representing potential digital evidence process

In this process, one should define procedures for pre-incident analysis of data representing potential digital evidence.

The input to this process includes the scenarios as defined in the scenario definition process as well as the output from the pre-incident gathering process. The input should also include the aims for the readiness processes.

The output of this process includes the defined activities for pre-incident analysis of the data that represent potential digital evidence. The aim of this analysis is to detect an incident. Therefore, activities defined in this process should include exact information on how the incident is detected and what behaviour constitutes an incident.

As the task of data analysis and incident detection is often outside the scope of the functionalities of targeted information systems, it is recommended that this process defines an interface between the readiness processes and a monitoring system, which would analyse data in order to detect incidents. The monitoring system can be any system that is specialized for this purpose. It can also be any one of the following systems: intrusion prevention systems, intrusion detection systems, change tracking systems, log processing systems, etc.

7.6 Planning incident detection process

In this process, one should define actions to be performed when an incident is detected. The output of this process includes defined actions to be performed once an incident is detected, in particular information to be passed on to the rest of digital investigation process. Information should also include pre-known system inputs, results from all of the readiness class processes, as well as data gathered and generated during the *implementation process group* processes.

7.7 Defining system architecture process

In this process, one should define information system architecture for the organization, while taking into account the output results of all previous readiness processes. The information system architecture in this context refer to the organizational structure of an information system, including necessary application systems, computer equipment, a communications network, and related software.

Input to this process is the result from all previous readiness processes. The input should also include the aims for the readiness processes.

The output of this process is the defined system architecture for the organization. The aim is to customize system architecture, with specific reference to electronic storage and transportation of data and/or information within the architecture, to accommodate the accomplishment of the aims of the readiness processes. The main aim of this process is to identify potential data and/or information sources within the system architecture.

7.8 Implementing system architecture process

In this process, one should implement the system architecture as defined in the *defining system architecture* process. The output of this process is the implemented system architecture.

Examples of *implementing system architecture* include the installation of new software, hardware, and/or policies which will permit the remainder of the readiness processes to be instantiated across the information system and the organization.

7.9 Implementing pre-incident gathering, storage, and handling of data representing potential digital evidence process

In this process, one should implement pre-incident gathering, storage, and handling of data representing potential digital evidence, as defined in the *planning pre-incident gathering, storage, and handling of data representing potential digital evidence* process. The output of this process is the implemented pre-incident gathering, storage, and handling of data representing potential digital evidence.

Examples of *pre-incident gathering, storage and handling of data representing potential digital evidence* include the implementation of logging software and hardware, with time stamping and digital signature mechanisms in place, or the implementation of customized software to gather the data of importance (i.e. system usage data).

7.10 Implementing pre-incident analysis of data representing potential digital evidence process

In this process, one should implement pre-incident analysis of data representing potential digital evidence, as defined in the *planning pre-incident analysis of data representing potential digital evidence* process. The output of this process is the implemented pre-incident analysis of data representing potential digital evidence.

Examples of *pre-incident analysis of data representing potential digital evidence* include the implementation of change-tracking software such as a file integrity checker, intrusion detection/prevention software and/or anti-virus software. As the output of this process is delivered in the form of detected incidents, this links to the input of the incident detection process of the digital investigation processes as listed in Figure 4.

7.11 Implementing incident detection process

In this process, one should implement the actions defined in the *planning incident detection* process. The implementation of incident detection depends also on and receives input from the *implementing pre-incident analysis of data representing potential digital evidence* process, as detection occurs based on the analysis performed.

During the *implementing incident detection* process, detection of an incident occurs according to the rules defined during *planning incident detection* process. Also, during the *implementing incident detection* process, one should decide on which data about the incident should be passed on to the rest of digital investigation process.

Examples of incident detection can be if change tracking software detects changes in a certain archived log or if an intrusion is detected via intrusion detection system.

Requirements for an event to be declared an incident requiring digital investigation would depend on policies of organization and cannot be prescribed by this International Standard.

This process represents an interface to the rest of the digital investigation process. This process is an overlap between readiness processes and an investigation itself. The reason for overlap is that the digital investigation cannot start until there is an incident detected.

7.12 Assessment of implementation process

In the *assessment of implementation* process, one performs an assessment of the results of the *implementation process group* and compares these to the aims for achieving digital investigation readiness. The output of this process is the results of the assessment of implementing digital investigation readiness for an information system. It is recommended that, at this process, a legal review is carried out for all procedures, controls, and architectures defined previously. The revision should show, amongst other, whether there is conformity with the legal environment and digital forensics principles of the particular jurisdiction, in order to assure admissibility of potential digital evidence in court.

7.13 Implementation of assessment results process

This process is concerned with the implementation of the conclusions from previous process. This process is optional, as it is possible that no changes are needed, based on the *assessment of implementation* process. Note that in Figure 4, this process is marked as optional and indicated as such with a dashed line around the process.

During this process, one should decide on recommendations for changes in one or more of the previous processes. The main decision here is whether to go back to one of the planning processes in the *planning processes group* of the *readiness class* of processes or to go back to one of the processes in the *implementation process group,* depending on the conclusions of the *assessment of implementation p*rocess. For example, one might conclude that the implementation of a certain measure (e.g. that during *implementing system architecture,* one has not properly implemented log-in authorization controls planned during the *defining system architecture* process) was not performed in an optimal manner or one might decide that new implementation as to be performed.

8 Initialization processes

8.1 Overview of initialization processes

The initialization processes class consists of processes that initialize the digital investigation by handling the first response of an incident and planning as well as preparing for the remainder of the incident investigation process. Figure 5 depicts the initialisation processes, including the

— incident detection process

— first response process

— planning process, and

— preparation process.

The concurrent processes in Figures 5, 6, and 7 are given for illustrative purposes and a detailed explanation of the concurrent processes will be discussed in Clause 11.

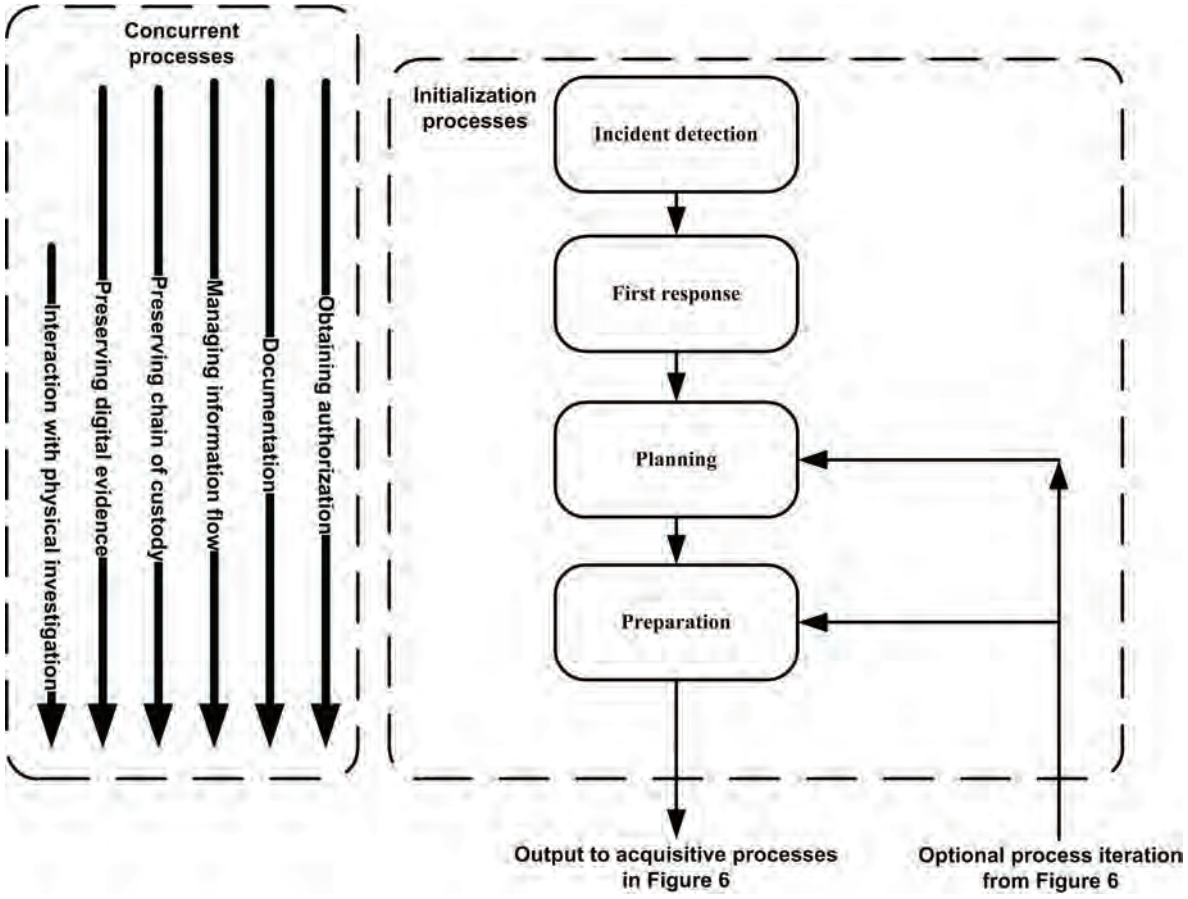

Figure 5 — Initialization processes

8.2 Incident detection process

Incident detection procedures should be in place prior to the beginning of this process. The procedures can define the relation between the information system where the incident might occur and the external incident detection system, which would have the task to detect an incident or can define how humans operating or administering information systems, detect an incident. Examples of external incident detection systems are intrusion detection systems, intrusion prevention systems, log-analysing systems, change-tracking systems, etc.

The incident detection process includes not only the detection of the incident, but also the classification and description of the incident, which has a significant influence on the rest of the process. For example, the digital investigation would take a completely different course if the incident was described as "unauthorized access to the root account of the operating system", than if it was described as 'using the computer to distribute abusive images'.

Based on the above, this process may consist of three sub-processes: incident detection, incident classification, and incident description.

It is important to note that the incident classification and incident description sub-processes should be performed based on information gathered prior to incident detection and should not include any activity

(e.g. running some data analysis software on the system) that might alter data at the information system in which incident has occurred, in order to preserve digital evidence.

NOTE The incident detection process is included in the digital investigation processes as a starting point. The reasoning behind defining the incident detection process as the first process, and not as a preparation or planning process is that digital investigation readiness activities should exist in a process separate to the rest of the digital investigation process. This is so because digital investigation practitioners can never ensure that each system they will be working or will have digital investigation readiness activities implemented. If preparation and planning for digital investigations would exist prior to incident detection, then this would be part of digital investigation readiness. Therefore, the actual digital investigation starts with *incident detection* and *first response*, followed by *preparation* and *planning* processes, which are concerned with the rest of the digital investigation process rather than with the digital investigation readiness process.

8.3 First response process

The *first response* process should include the first response to the detected incident. Also see ISO/IEC 27037 for more information on incident response. Depending on the type and severity of the incident, this might include disconnecting equipment from a networked environment, detecting corrupted data, etc. It is required that the first response does not have a negative influence on the possibility to perform a digital investigation, e.g. to avoid powering off the equipment, opening or changing files on a live system etc.

Defining the *first response* sub-processes is out of the scope of this International Standard, as these can vary greatly depend on the type of target information systems, data contained in the target information system, circumstances of the incident, classification and description of the incident, etc.

The *first response* process is included as a process because it falls within the scope of any digital investigation since such a process will assure the integrity of potential digital evidence.

8.4 Planning process

During this process, the investigator has to perform all the potential planning needed for later in the digital investigation process. Planning should include the use of defined ISO/IEC 27041 based validated processes to develop relevant procedures and methodologies to be used, planning for use of appropriate human resources. and the planning of all activities during other processes.

If digital investigation readiness controls were implemented, the investigator should plan how to use the results of those controls so as to maximize the success of the digital investigation process. The aims of the digital investigation readiness process are to maximize the potential use of potential digital evidence, minimize the costs of the investigation, minimize interference with and prevent the interruption of business processes, and to preserve or improve the current level of information systems security.

The planning process is included because it is of extreme importance due to the fact that it determines the efficiency and success of all the other processes.

8.5 Preparation process

Preparation process activities are intended to prepare an organization for performing activities within this process that might include — but is not limited to — the preparation of relevant equipment (hardware and software), infrastructure, human resources, raising awareness, training, and documentation. During this process, preparations also have to be made to implement procedures defined in the previous process.

This process is included since such a process will ensure that the investigator is better prepared in order to carry out the acquisitive processes in a more efficient manner. This will also ensure that the integrity of potential digital evidence is not compromised due to possible ill-preparedness by the investigator.

9 Acquisitive processes

9.1 Overview of acquisitive processes

The acquisitive processes class consists of processes that are concerned with acquisition of potential digital evidence. Figure 6 depicts the acquisitive processes, including the

— potential digital evidence identification process,

— potential digital evidence collection process,

— potential digital evidence acquisition (optional),

— potential digital evidence transportation process, and

— potential digital evidence storage process.

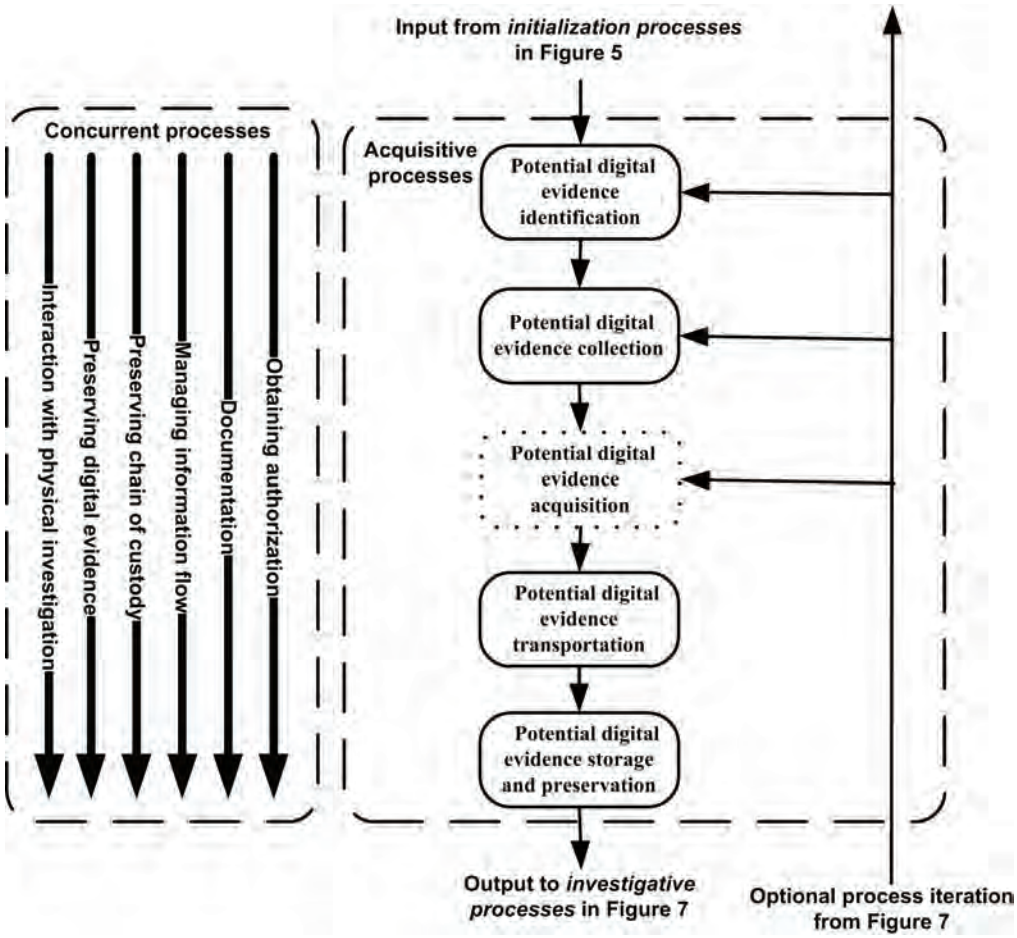

Figure 6 — Acquisitive processes

9.2 Potential digital evidence identification process

This is the second process performed at the scene of the incident. Although it overlaps in time with the previous process, it should be considered as a separate process because it includes different types of procedures within the process, with the specific aim of identifying potential digital evidence.

Identifying potential digital evidence at the incident scene is of crucial importance for the remainder of the process, because if potential digital evidence is not identified at this point, it might not even exist at a later point during the process. This is especially important when an incident happens in a networked

environment, in an environment where live investigations should be performed, in a cloud environment or in an environment with exceptionally large amounts of data to deal with.

This process is included with the sole aim to identify potential digital evidence.

9.3 Potential digital evidence collection process

Once potential digital evidence has been identified, it has to be collected in order to permit its analysis in a later process.

Potential digital evidence must be collected in such a manner that its integrity is preserved. This is important if one needs to use this evidence at a later stage to draw some formal conclusions, i.e. in a court of law. Adhering to strict legal regulations during the evidence collection process is of crucial importance, as digital evidence might become unusable when proper procedures are not followed.

9.4 Potential digital evidence acquisition process

Once potential digital evidence has been collected, it has to be acquired in order to permit its analysis in a later process.

Proper data acquisition of protected devices with additional security controls such as data encryption should be considered. Guidance on this, and sound processes for handling potential digital evidence, is found in ISO/IEC 27037. Adhering to strict legal regulations during the potential digital evidence acquisition process is of crucial importance, as potential digital evidence might become unusable when proper procedures are not followed.

It is common practice to make verifiable images (see ISO/IEC 27037) using hash functions (see ISO/IEC 10118-2) of all the bits contained within each media item that contains potential digital evidence.

Professionals and scientists in the digital investigation field have a task to develop proper procedures for the acquisition of potential digital evidence that is applicable to networked environments, the live investigation process, cloud environments, and environments with large amounts of data.

Take note that this process is optional at this stage, since it is not always possible to acquire one or more images of the evidence after it has been collected. It often happens that the image acquisition only takes place within an investigation laboratory and, hence, this process might only occur within the investigative processes class. Although this process is marked as optional at this stage as well as within the investigative processes class, it is imperative that exactly one instance of the process is carried out, i.e. either here or within the investigative processes class. This process, as described in this clause, is exactly the same as the first process within the investigative processes class and is not described again within the investigative processes class.

9.5 Potential digital evidence transportation process

During this process, potential digital evidence is to be transported to a location where it is to be stored and later analysed. Transportation can be done physically or electronically. If the evidence is transported electronically, special precautions have to be taken to preserve the integrity and chain of custody, such as encrypting and digitally signing data.

9.6 Potential digital evidence storage and preservation process

The storage of potential digital evidence might be needed if analysis cannot be performed right away or if there is a legal requirement to keep potential digital evidence for a certain period of time.

Preservation of the integrity of the evidence and chain of custody is of utmost importance during this process. Care should also be taken not to damage the media containing potential digital evidence due to shock, temperature, humidity, pollution, loss of power, malfunction, etc.

10 Investigative processes

10.1 Overview of investigative processes

The investigative processes class consists of processes that are concerned with investigating the incident that is the cause of the digital investigation and is concerned with analysing the evidence, interpreting results from the analysis, reporting on results of the *digital evidence interpretation* process and presenting these results in a court of law or to the relevant parties involved. Finally, the digital investigation draws to a close within the *investigation closure* process. Figure 7 depicts the investigative processes, including the

— potential digital evidence acquisition (optional),

— potential digital evidence examination and analysis process,

— digital evidence interpretation process,

— reporting process,

— presentation process, and

— investigation closure process.

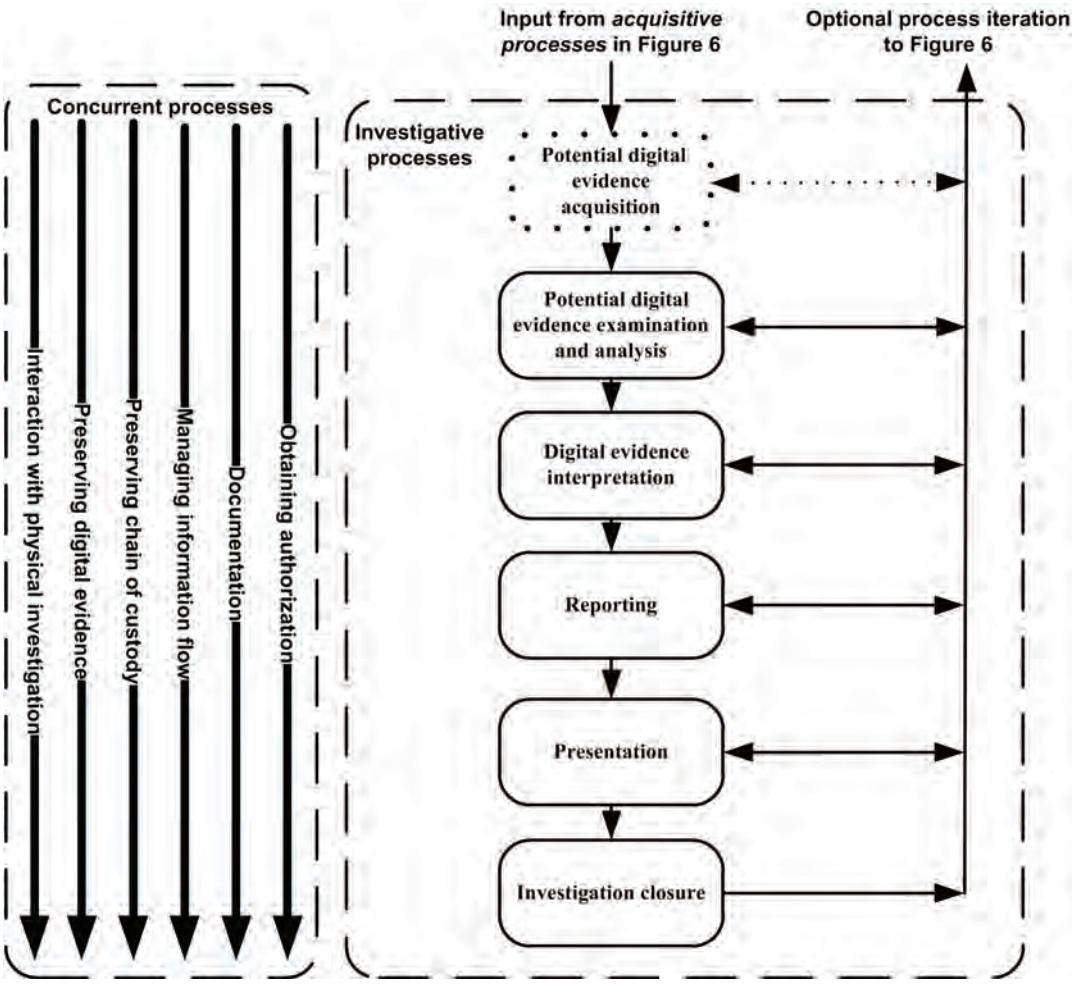

Figure 7 — Investigative processes

10.2 Potential digital evidence acquisition process

See 9.4 for a description of this process.

10.3 Potential digital evidence examination and analysis process

Examination and analysis of the digital evidence involves the use of a large number of techniques to identify digital evidence as well as reconstructing it, if needed. In order to make a hypothesis on how the incident occurred, one should define what its exact characteristics are and who is to be held responsible. Making a hypothesis basically involves the reconstruction of a sequence of events that have led to the current state of the system being investigated. Due to the volume, diversity and complexity of the data to be analysed in present-day digital investigations, the analysis of evidence becomes a challenge.

As volumes of data to be examined and analysed can be vast, accredited automated techniques are often employed to complement manual validation techniques.

See ISO/IEC 27042 for details on the digital evidence analysis process.

It should be noted that from this point onwards, "potential digital evidence" becomes "digital evidence" according to the definitions of 'potential digital evidence' and 'digital evidence'.

10.4 Digital evidence interpretation process

The results from the *potential digital evidence examination and analysis* process should then be interpreted. Interpretation of any evidence is dependent on the information available about the circumstances surrounding the creation of that item of digital evidence. To be able to carry out a proper interpretation, information from persons involved in the day-to-day running of the system(s) which are being investigated, is often required. Furthermore, information about the purpose of the investigation and a definition of the scope of the investigation is also required.

One goal of the *digital evidence interpretation* process is to use scientifically proven methods to construct explanations for the presence of the digital artefacts identified as well as likelihood estimates for each investigation during the *potential digital evidence examination and analysis* process, within the context of the investigation. If the contextual information changes, the interpretation may also have to change in order to reflect changes to the contextual information. A further goal of the digital evidence interpretation process is to classify the interpreted evidence according to relevance. This means that the evidence, as interpreted, is organized in such a way that it is distinguished which digital evidence artefacts are more important than others. The decision process on deciding which pieces of digital evidence would be more important than others is left to the discretion of one or more competent investigators.

See ISO/IEC 27042 for details on the digital evidence interpretation process.

10.5 Reporting process

The interpretation that results from the *digital evidence interpretation* process forms the main output, i.e. the report. The report should, where economical, be printed on paper. It is possible that during a certain digital investigation, the number of digital evidence artefacts could be many. Therefore, due diligence should be exercised to list all relevant digital evidence in the report in order to assure that no valuable evidence is omitted from the report.

The report should be written in simple language and should be clear, concise and unambiguous in its statements. It should also be understandable for a wide audience whom do not necessarily possess a technical understanding of incident investigations. Such audiences include, but not limited to, judges, juries, the accused, lawyers, prosecutors, an organization's management team, shareholders, and employees.

The author(s) of a report should always be aware of the potential impact of the report in a law suit on all the applicable audiences as mentioned above. Authors of such reports should also keep in mind possible consequences of potentially wrong or misinterpreted reports. Therefore, the report should elaborate on issues such as which potential evidence was collected/acquired, which analysis techniques were

performed, which statements and from whom have been taken into account and what outcome results from this. Sometimes no clear outcome is possible based on the available evidence. In such a case, the report should state clearly the assumptions made, the probabilities corresponding to the assumptions and the conclusions arising from the assumptions. It is essential to emphasize the hypothetical character of such conclusions.

10.6 Presentation process

The document created during the *reporting* process is to be presented to a wide audience as stated in this Clause. The main purpose of the *presentation* process is to conduct a live demonstration of the results based on the report. This demonstration can be performed using questions and answers, as an oral presentation, as a multimedia presentation, as an expert witness testimony or as whatever is suitable to the case.

The *presentation* process also includes proving the validity of the hypothesis if or when the hypothesis is challenged. Thus, the one who presents the hypothesis should be well prepared for it and should preferably have had insight into the *reporting* process.

10.7 Investigation closure process

This process concludes the investigation and a decision is to be recorded on the validity of the hypothesis set in the presentation process. The digital investigation process is iterative. This implies that — after completing this process — one can go back to any of the earlier processes that follow the *first response* process.

The closing process should include the following sub-processes:

— deciding on need to iterate to a previous process;

— record acceptance or rejection of the hypothesis;

— returning evidence, if needed;

— destruction of evidence, if needed. There are various laws in different jurisdictions. The way in which evidence is destroyed, or whether it is destroyed at all, or whether it needs to be stored for a certain period of time after the case has been completed, all depends on the local laws. The investigator should take cognisance of this. More information on the destruction of data can be found in ISO/IEC 27040. More information on storage of data can be found in ISO 15489-1;

— distribution of relevant information to all stakeholders (i.e. communicating the need to iterate to a previous process, deciding on the acceptance or rejection of the hypothesis, or providing any reports or documents from the *presentation* process);

— project debriefing and lessons learned.

11 Concurrent processes

11.1 Overview of the concurrent processes

In addition to the digital investigation processes classes (i.e. the readiness, initialization, acquisitive, and investigative processes classes), a number of processes (i.e. the concurrent processes class) exist that take place alongside with these digital investigation processes. These processes include the

— obtaining authorization process,

— documentation process,

— managing information flow process,

— preserving chain of custody process,

— preserving digital evidence process, and

— interaction with physical investigation process.

Concurrent processes are defined as the principles which should be applied throughout the digital investigation process since such concurrent processes are applicable to many other processes within the digital investigation process. For example, *documentation* is a concurrent process that is applicable to all processes within the digital investigation process, since all tasks carried out during the entire digital investigation process should be thoroughly logged and documented.

The concurrent processes suggested above are justified, since the principles of the digital investigation process, as well as the preservation of the evidence and chain of custody, should be translated into actionable items. These processes should run concurrently with all other processes in order to assure full admissibility of the digital evidence in a court of law. Moreover, legacy processes (such as *obtaining authorization*, *documentation,* and *interaction with the physical investigation*) should actually run across several or all processes. The aim of these concurrent processes is to achieve higher efficiency of the investigation. Information flow should also be defined as a separate concurrent process.

The concurrent processes are explained next.

11.2 Obtaining authorization process

Proper authorization should be obtained for each process performed within all of the digital investigation processes. Authorization might be required from government authorities, system owners, system custodians, principals, users etc. It is important to obtain proper authorization for actions performed during the digital investigation process in order not to infringe on the rights of system owners, custodians, principals, or users, but also to assure that no legal rule is infringed. Needed authorizations would depend on the environment where the digital investigation is performed, both within the legal and the organizational environment.

11.3 Documentation process

Each process performed should be documented in order to assure repeatability and reproducibility, preserve chain of custody, but also to improve efficiency and a higher probability of a successful digital investigation. Proper documentation should also be demonstrated during the presentation process.

This process should include incident scene documentation which is performed at the scene of the incident, if applicable, and involves the proper documentation of the complete incident scene, including written documentation of activities, sketches, photographs, videos, and labelling the potential digital evidence. All activities performed in relation to the digital investigation processes should be recorded, together with details on the architecture and components of the information system where the incident occurred, if applicable.

11.4 Managing information flow process

A defined information flow should exist between each of the processes and among different stakeholders. This information flow has to be defined for each type of investigation. It is important to identify and describe information flows so that they can be secured and supported technologically. For instance, an information flow could refer to the exchange of digital evidence between two investigators involved in the same investigation. Protection of this information flow can be in the form of, for example, the use of trusted PKI and time stamping to identify the different investigators and authenticate evidence (protecting its integrity), as well as to protect the confidentiality of the evidence.

11.5 Preserving chain of custody process

All legal requirements should be complied with and all processes should be properly documented in order to preserve chain of custody as the evidence is handled by several parties. This process is to be performed from the *incident detection* process until the last process.

11.6 Preserving digital evidence process

Preserving digital evidence means to preserve the integrity of the original digital evidence. In order to achieve this, one should conform to strict procedures from the time that the incident is detected until such time as the investigation is closed. These procedures should ensure that the original evidence is not changed and, even more important, they should guarantee that no opportunity arises during which the original evidence may be changed, lost, stolen, destroyed, etc.

11.7 Interaction with physical investigation process

The digital investigation process can be dependent on and interconnected with the physical investigation, if such an investigation is conducted in relation to the same incident. Therefore, this activity should define the relationship between the digital investigation process and the physical investigation. The interaction is important for preserving the chain of custody, preserving the integrity of the digital evidence, protecting the digital evidence from damage, and ensuring an efficient investigation according to the investigator's needs and fast adaption to changing boundaries, scope, or investigation objectives.

12 Digital investigation process model schema

Figure 8 represents the entire digital investigation processes, combining Figures 4 to 7 in order to view the digital investigation process in its totality. As mentioned earlier, note that the processes are sequential — with the exception of evidence identification process, which may overlap in time. Also, note that not all concurrent processes run concurrently with all other processes. For instance, *preserving chain of custody* and *preserving digital evidence interaction* concurrent processes start only with the *implementing pre-incident collection, storage, and handling of data representing potential digital evidence* process. However, these are not performed during *assessment process group* in *readiness class* of processes. Also, *interaction with physical investigation* process starts only with *first response* process.

The digital investigation processes are iterative, which implies that after the last process one can return to previous process. Note, however, that iteration is optional and that one can only return to certain processes, as shown on Figure 8. One can only go back to *planning* process, *preparation* process, *potential digital evidence identification* process, *potential digital evidence acquisition* process, *digital evidence analysis* process, *digital evidence interpretation* process, *reporting* process, *or presentation* process.

What follows is a list of examples when processes can be iterative:

a) When, during the *investigation closure* process, it is noted that there is a need for additional digital evidence and that not all potential digital evidence were identified, one would go to the *potential digital evidence identification* process.

b) When, during the *investigation closure* process, it is noted that there is a need for additional examination and analysis or interpretation of digital evidence, for the reason that hypothesis presented cannot be adopted by stakeholders, one would go back to *digital evidence analysis* or *digital evidence interpretation* process.

c) When, during the *investigation closure* process it is noted that digital investigation findings were not presented up to the standard requested, one would go back to either *reporting process* or *presentation* process.

Take note that the above list of examples is neither comprehensive nor exclusive.

NOTE The *preserving chain of custody* and *preserving digital evidence* processes within the *concurrent processes* class in Figure 8 do not run concurrently with the following two processes within the readiness processes class: *assessment of implementation* and *implementation of assessment results*. For clarity, see Figure 4 again.

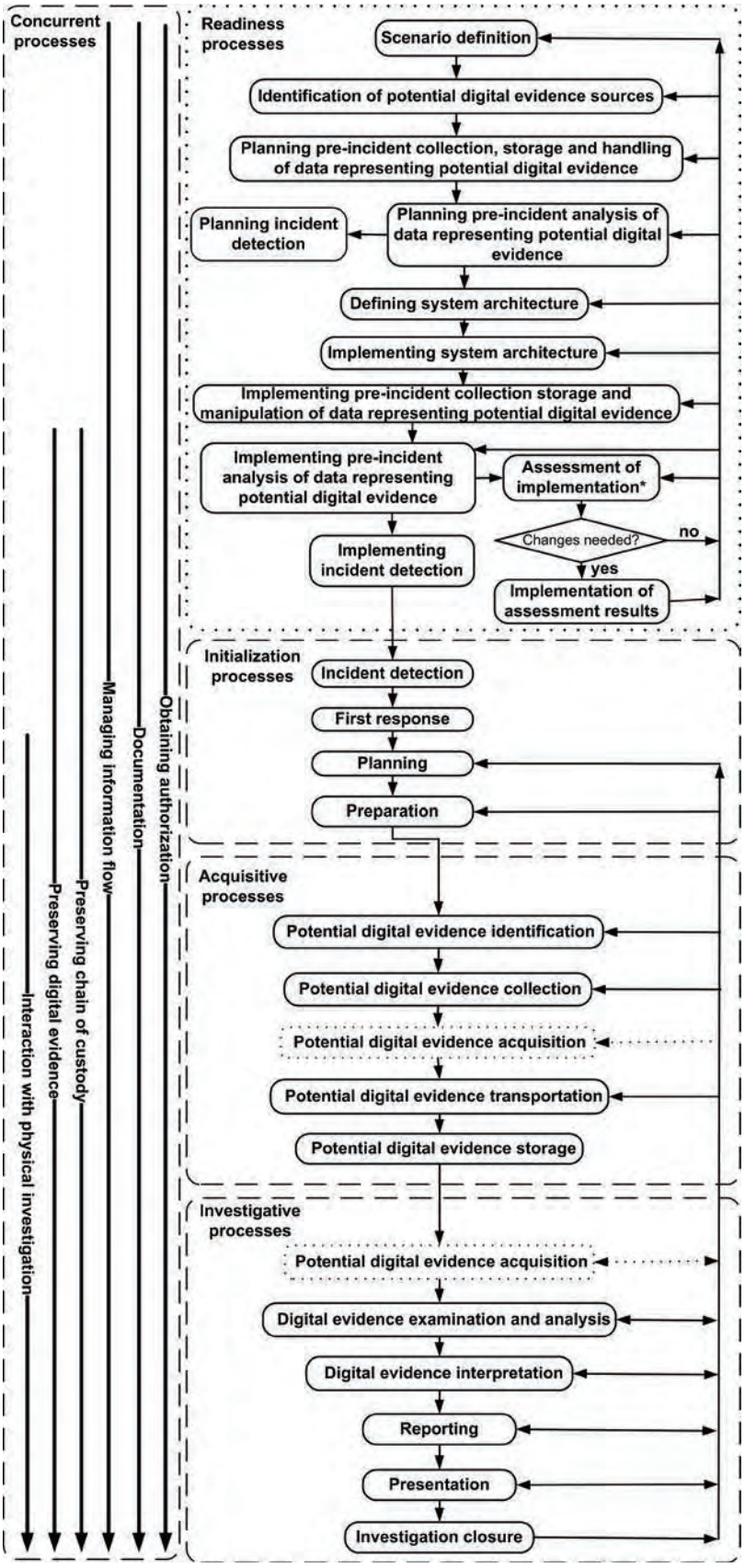

Figure 8 — Harmonized digital investigation process schema

Annex A
(informative)

Digital investigation processes: motivation for harmonization

Based on numerous currently-published digital investigation process models,[3] to [17] there exist clear disparities among such digital investigation process models by the time of writing this International Standard. Disparities include: different number of investigation processes included, different scope of process models, different scope of the processes with the same names within different process models, different hierarchy levels and even different concepts applied to the construction of the process model (e.g. most of the models are based on a physical crime investigation processes).

Processes have been selected based on previous work[3] to [17] in this field in order to harmonize the digital investigation processes. Existing models are compared with the harmonized digital investigation process model in Table A.1. The harmonized model is mapped to existing models in a bid to show how it compared with existing models by the time of writing this International Standard. This also serves as further motivation why the harmonized digital investigation process model should be standardized.

The harmonized model is iterative and multi-tiered. Sub-processes of the model are not shown on the comparison table for the sake of simplicity of view. Each mapped process starts with a number, marking a sequence of processes within the model with which comparison is being made.

Ideally, all planning of activities (planning, defining of the approach strategy, defining of the response strategy, etc.) should be done prior to the incident — thus during the planning process.

Based on the comparison made in Table A.1, the comprehensiveness of the harmonized model should be trivial. The “concurrent processes” principle is also introduced, as it would assure higher efficiency and digital evidence admissibility. Note also that the order of the processes differs from some of the previous models and that the order makes provision for a more efficient process, such as that a digital investigation readiness process should be kept separate from the digital investigation process. Incident detection and first response should be included in the digital investigation process model.

The harmonized digital investigation process model is comprehensive and inclusive of all the benefits conveyed by previous models. The processes in the proposed model are well defined in terms of scope, functions and order. Several processes to be performed are also provided which operates concurrently with the initial processes of the model, in order to achieve efficiency of investigation and ensure the best possible admissibility of digital evidence. These processes provide the principles in digital investigations.

Use of the harmonized digital investigation process model should bring about multiple benefits. A first benefit would be the higher admissibility of digital evidence in a court of law, due to the fact that a standardized process was followed. Also, human error and omissions during the digital investigation process would be minimized once such a harmonized process model was used.

Usage of the model across national borders should enable modern society to fight cybercrime far more efficiently, and interaction between private and government entities should also be made much easier and more efficient. Last, but not least, the digital investigation process should ultimately enhance the efficiency, effectiveness, and robustness of digital investigations.

Table A.1 — Comparison of existing models and the harmonized model

	The harmonized model	DFWRS[1][18]	Reith et al.[3]	DOJ[4]	Carrier et al.[5]	Mandia et al.[7]	Beebe et al.[8]	Cuardhuain[17]	Cohen[9]	Casey and Rose[19]	ACPO[20]
Process											
1.	Incident detection	1. Identification	1. Identification		2. Detection and notification	2. Detection of the incident 3. Initial response	2. Incident response	1. Awareness			
2.	First response					3. Initial response	2. Incident response				2.1 Secure and control the crime scene
3.	Planning		3. Approach strategy		1. Readiness group of phases	4. Response strategy formulation		3. Planning			1. Preparations for investigation
4.	Preparation		2. Preparation	1. Preparation	1. Readiness group of phases	1. Pre-incident preparation	1. Preparation				1. Preparations for investigation
5.	Potential digital evidence identification		6. Examination	2. Recognition and identification	4.2 Survey for digital evidence			5. Search for and identify evidence	1. Identification	1.Gather information and make observations	5.1 The collection process
6.	Potential digital evidence acquisition	2. Preservation 3. Collection	4. Preservation 5. Collection	4. Collection and preservation	4.1 Preservation of digital crime scene	5. Duplication 7. Secure measure implementation 8. Network monitoring	3. Data collection	6. Collection of evidence	2. Collection 3. Preservation	1.Gather information and make observations	2.3 Initial collecting of volatile data 5.1 The collection process
7.	Potential digital evidence transportation			5. Packaging and transportation				7. Transport of evidence	4. Transportation		3. Transport
8.	Potential digital evidence storage							8. Storage of evidence	5. Storage		4. Storage
9.	Digital evidence examination and analysis	4. Examination 5. Analysis	7. Analysis	6. Examination 7. Analysis	4.4 Search for digital evidence	6. Investigation	4. Data analysis	9. Examination of evidence	6. Analysis		5.2 The analysis process

Table A.1 — *(continued)*

	The harmonized model	DFWRS[1][18]	Reith et al.[3]	DOJ[4]	Carrier et al.[5]	Mandia et al.[7]	Beebe et al.[8]	Cuardhuain[17]	Cohen[9]	Casey and Rose[19]	ACPO[20]
Process											
10.	Digital evidence interpretation				4.5 Digital crime scene reconstruction			10. Hypothesis	7. Interpretation 8. Attribution 9. Reconstruction	2. Form hypothesis to explain observations, 3.Evaluate the hypothesis, 4. Draw conclusions and communicate findings.	5.3 The examination process
11.	Reporting			8. Report		10. Reporting					5.4 The reporting process
12.	Presentation	6. Presentation	8. Presentation	8. Report	4.6 Presentation of digital scene theory	10. Reporting	5. Findings presentation	11. Presentation of hypothesis 12. Proof/defence of hypothesis	10. Presentation	4 .Draw conclusions and communicate findings.	5.4 The reporting process
13.	Investigation closure	7. Decision	9. Returning evidence			9. Recovery 11. Follow-up	6. Closure	13. Dissemination of information	11. Destruction		6. Disclosure

Table A.1 — *(continued)*

	The harmonized model	DFWRS[1][18]	Reith et al.[3]	DOJ[4]	Carrier et al.[5]	Mandia et al.[7]	Beebe et al.[8]	Cuardhuain[17]	Cohen[9]	Casey and Rose[19]	ACPO[20]
Concurrent processes											
1.	Interaction with physical investigation				3. Physical crime scene investigation group of phases						As principle and set of processes, including preservance of physical evidence and interviews
2.	Preserving chain of custody	As principle	As principle	As principle	As principle	As principle	As principle	As principle	As principle	As principle	As principle
3.	Preserving digital evidence	As principle	As principle	As principle	As principle	As principle	As principle	As principle	As principle	As principle	As principle
4.	Managing information flow							Described			Partially described
5.	Documentation	As principle	As principle	As principle	As principle	As principle	As principle	As principle	As principle	As principle	As principle
6.	Obtaining authorization				2. Confirmation and authorization process			2. Authorization			As principle

NOTE Fields marked with "As principle" indicate that the referenced work contains the notion of a principle that is a basis for a specific concurrent process. For example, a principle that proper authorization should be obtained for certain processes and/or actions is a basis for obtaining authorization for concurrent process.

Bibliography

[1] Palmer G. A Road Map for Digital Forensic Research". Technical Report DTR-T001-01, DFRWS, Report from the First Digital Forensic Research Workshop (DFRWS), 2001

[2] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993)

[3] Reith M., Carr C., Gunsch G. An examination of digital forensic models", International Journal of Digital Evidence, 2002

[4] The U.S. Department of Justice. Electronic Crime Scene Investigation- A Guide for First Responders, 2001

[5] Carrier B., & Spafford E. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence. 2003, **2** p. 2 [Electronic version]

[6] Carrier B., & Spafford E. An Event-Based Digital Forensic Investigation Framework. Digit. Invest. 2005, **2** (2)

[7] Mandia Kevin, Prosise Chris, Pepe Matt "Incident Response & Computer Forensics" (Second Ed.), McGraw-Hill/Osborne, Emeryville, 2003

[8] Beebe N.L., & Clark J.G. A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. Digit. Invest. 2005, **2** (2)

[9] Cohen Frederick B. "Fundamentals of Digital Forensic Evidence, Chapter in Handbook of Information and Communication Security", 2010, accessed at all.net on 04.01.2011

[10] Cohen Frederick B., Lowrie Julie, Preston Charles The State of the Science of Digital Evidence Examination", 2011, all.net

[11] Leigland R., & Krings A. A Formalization of Digital Forensics", International Journal of Digital Evidence, Fall 2004, Volume 3, Issue 2

[12] Hankins Ryan, Uehara T., Liu J A Comparative Study of Forensic Science and Computer Forensics", Third IEEE International Conference on Secure Software Integration and Reliability Improvement, 2009

[13] Committee on Identifying the Needs of the Forensic Sciences Community. Strengthening Forensic Science in the United States: A Path Forward", ISBN: 978-0-309-13130-8, 254 pages. Committee on Applied and Theoretical Statistics, National Research Council, 2009

[14] Scientific Working Group on Digital Evidence (SWGDE). Position on the National Research Council Report to Congress — Strengthening Forensic Science in the United States: A Path Forward, 2009

[15] Garfinkel S., Farrella P., Roussev V., Dinolt G. Bringing science to digital forensics with standardized forensic corpora. Digit. Invest. 2009, **6** pp. S2–S11

[16] Pollitt M. Applying Traditional Forensic Taxonomy to Digital Forensics", Advances in Digital Forensics IV, IFIP TC11.9 Conference Proceedings, 2009

[17] Séamus Ó., & Ciardhuáin An Extended Model of Cybercrime Investigations", International Journal of Digital Evidence, Summer 2004, Volume 3, Issue 1

[18] Palmer G. A Road Map for Digital Forensic Research". Technical Report DTR-T001-01, DFRWS, Report From the First Digital Forensic Research Workshop (DFRWS), 2001

[19] Casey Eoghan, & Rose Curtis W. Forensic Analysis" in "Handbook of Digital Forensics and Investigation", 2010

[20] "ACPO Good Practice Guide for Computer-Based Evidence", http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf, 2008

[21] Rowlingson Robert A Ten Step Process for Forensic Readiness", International Journal of Digital Evidence, Volume 2, Issue 3, 2004

[22] Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council. Strengthening Forensic Science in the United States: A Path Forward. National Academies Press, 2009

[23] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[24] ISO 15489-1, *Information and documentation — Records management — Part 1: General*

[25] ISO/IEC 10118-2, *Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher*

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

[27] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

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

[29] ISO/IEC 27035 (all parts), *Information technology — Security — Information security incident management*[1)]

[30] ISO/IEC 27037:2012, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[31] ISO/IEC 27038, *Information technology — Security techniques — Specification for digital redaction*

[32] ISO/IEC 27040, *Information technology — Security techniques —Storage Security*

[33] ISO/IEC 27041:—, *Information technology — Security techniques — Guidance on assuring the suitability and adequacy of investigative methods*[2)]

[34] ISO/IEC 27042:—, *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*[3)]

[35] ISO/IEC 27044, *Guidelines for Security Information and Event Management (SIEM)*[4)]

[36] ISO/IEC 27050 (all parts), *Information technology — Security techniques — Electronic discovery*[5)]

[37] ISO/IEC 30121, *System and software engineering — Information technology — Governance of digital forensic risk framework*

[38] ILAC-G19, Guidelines for forensic science laboratories

[40] Valjarevic A., & Venter H.S. Harmonised Digital Forensic Investigation Process Model", International workshop on Digital Forensics in the Cloud (IWDFC), South Africa, 2012

1) Under preparation.

2) To be published.

3) To be published.

4) Under preparation.

5) Under preparation.

[41] Valjarevic A., & Venter H.S. Analyses of the State-of-the-art Digital Forensic Investigation Process Models", The Southern Africa Telecommunication Networks and Applications Conference (SATNAC), South Africa, 2012

[42] Valjarevic A., & Venter H.S. Towards a Harmonized Digital Forensic Investigation Readiness Process Model", Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, 2013

[43] ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*

ICS 35.040

Price based on 30 pages