INTERNATIONAL STANDARD

ISO/IEC 27035-1

Second edition
2023-02

Information technology — Information security incident management —

Part 1: Principles and process

Technologies de l'information — Gestion des incidents de sécurité de l'information —

Partie 1: Principes et processus

Reference number
ISO/IEC 27035-1:2023(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27035-1:2016), which has been technically revised.

The main changes are as follows:

— the title has been modified;

— new terms “incident management team” and “incident coordinator” are defined in Clause 3;

— new subclauses 4.5, 4.6 and 4.7 are added in Clause 4;

— the title of Clause 5 has been changed to “Process”;

— Annex C has been updated;

— a new Annex D has been added;

— the text has been editorially revised.

A list of all parts in the ISO/IEC 27035 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The ISO/IEC 27035 series provides additional guidance to the controls on incident management in ISO/IEC 27002. These controls should be implemented based upon the information security risks that the organization is facing.

Information security policies or controls alone do not guarantee total protection of information, information systems, services or networks. After controls have been implemented, residual vulnerabilities are likely to remain that can reduce the effectiveness of information security and facilitate the occurrence of information security incidents. This can potentially have direct and indirect adverse consequences on an organization's business operations. Furthermore, it is inevitable that new instances of previously unidentified threats cause incidents to occur. Insufficient preparation by an organization to deal with such incidents makes any response less effective, and increases the degree of potential adverse business consequence. Therefore, it is essential for any organization desiring a strong information security programme to have a structured and planned approach to:

— plan and prepare information security incident management, including policy, organization, plan, technical support, awareness and skills training, etc.;

— detect, report and assess information security incidents and vulnerabilities involved with the incident;

— respond to information security incidents, including the activation of appropriate controls to prevent, reduce, and recover from impact;

— deal with reported information security vulnerabilities involved with the incident appropriately;

— learn from information security incidents and vulnerabilities involved with the incident, implement and verify preventive controls, and make improvements to the overall approach to information security incident management.

The ISO/IEC 27035 series is intended to complement other standards and documents that give guidance on the investigation of, and preparation to investigate, information security incidents. The ISO/IEC 27035 series is not a comprehensive guide, but a reference for certain fundamental principles and a defined process that are intended to ensure that tools, techniques and methods can be selected appropriately and shown to be fit for purpose should the need arise.

While the ISO/IEC 27035 series encompasses the management of information security incidents, it also covers some aspects of information security vulnerabilities. Guidance on vulnerability disclosure and vulnerability handling by vendors is also provided in ISO/IEC 29147 and ISO/IEC 30111, respectively.

The ISO/IEC 27035 series also intends to inform decision-makers when determining 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.

Further information about investigative standards is available in Annex A.

Information technology — Information security incident management —

Part 1: Principles and process

1 Scope

This document is the foundation of the ISO/IEC 27035 series. It presents basic concepts, principles and process with key activities of information security incident management, which provide a structured approach to preparing for, detecting, reporting, assessing, and responding to incidents, and applying lessons learned.

The guidance on the information security incident management process and its key activities given in this document are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance according to their type, size and nature of business in relation to the information security risk situation. This document is also applicable to external organizations providing information security incident management services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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, definitions and abbreviated terms

3.1 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1.1
incident management team
IMT
team consisting of appropriately skilled and trusted members of an organization responsible for leading all information security incident management activities, in coordination with other parties both internal and external, throughout the incident lifecycle

Note 1 to entry: The head of this team can be called the incident manager who has been appointed by top management to adequately respond to all types of incidents.

3.1.2
incident response team
IRT
team of appropriately skilled and trusted members of an organization that responds to and resolves incidents in a coordinated way

Note 1 to entry: There can be several IRTs, one for each aspect of the incident.

Note 2 to entry: Computer Emergency Response Team (CERT[1)]) and Computer Security Incident Response Team (CSIRT) are specific examples of IRTs in organizations and sectorial, regional, and national entities wanting to coordinate their response to large scale ICT and cybersecurity incidents.

3.1.3
incident coordinator
person responsible for leading all *incident response* (3.1.9) activities and coordinating the *incident response team* (3.1.2)

Note 1 to entry: An organization can decide to use another term for the incident coordinator.

3.1.4
information security event
occurrence indicating a possible breach of information security or failure of controls

3.1.5
information security incident
related and identified *information security event(s)* (3.1.4) that can harm an organization's assets or compromise its operations

3.1.6
information security incident management
collaborative activities to handle *information security incidents* (3.1.5) in a consistent and effective way

3.1.7
information security investigation
application of examinations, analysis and interpretation to aid understanding of an *information security incident* (3.1.5)

[SOURCE: ISO/IEC 27042:2015, 3.10, modified —"information security" was added to the term and the phrase "an incident" was replaced by "an information security incident" in the definition.]

3.1.8
incident handling
actions of detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (3.1.5)

3.1.9
incident response
actions taken to mitigate or resolve an *information security incident* (3.1.5), including those taken to protect and restore the normal operational conditions of an information system and the information stored in it

3.1.10
point of contact
PoC
defined organizational function or role serving as the coordinator or focal point of information concerning incident management activities

Note 1 to entry: The most obvious PoC is the role to whom the information security event is raised.

1) CERT is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of this product.

3.2 Abbreviated terms

BCP	business continuity planning
CERT	computer emergency response team
CSIRT	computer security incident response team
DRP	disaster recovery planning
ICT	information and communications technology
IMT	incident management team
IRT	incident response team
ISMS	information security management system
PoC	point of contact
RPO	recovery point objective
RTO	recovery time objective

4 Overview

4.1 Basic concepts

Information security events and incidents may happen due to several reasons:

— technical/technological, organizational or physical vulnerabilities, partly due to incomplete implementations of the decided controls, are likely to be exploited, as complete elimination of exposure or risk is unlikely;

— humans can make errors;

— technology can fail;

— risk assessment is incomplete and risks have been omitted;

— risk treatment does not sufficiently cover the risks;

— changes in the context (internal and/or external) so that new risks exist or treated risks are no longer sufficiently covered.

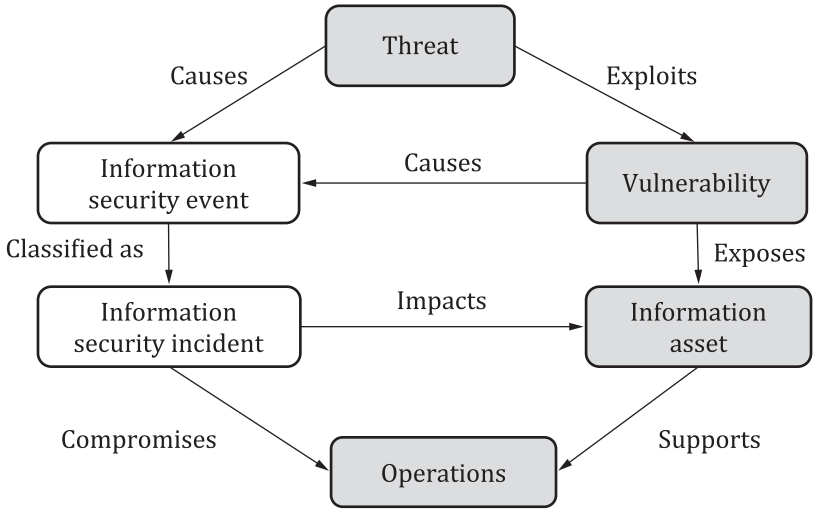
The occurrence of an information security event does not necessarily mean that an attack has been successful or that there are any implications on confidentiality, integrity or availability, i.e. not all information security events are classified as information security incidents.

Information security incidents can be deliberate (e.g. caused by malware or breach of discipline), accidental (e.g. caused by inadvertent human error) or environmental (e.g. caused by fire or flood) and can be caused by technical (e.g. computer viruses) or non-technical (e.g. loss or theft of hardcopy documents) means. Incidents can include the unauthorized disclosure, modification, destruction, or unavailability of information, or the damage or theft of organizational assets that contain information.

Annex B provides descriptions of selected examples of information security incidents and their causes for informative purposes only. It is important to note that these examples are by no means exhaustive.

A threat exploits vulnerabilities (weaknesses) in information systems, services, or networks, causing the occurrence of information security events and thus potentially causing incidents to information

assets exposed by the vulnerabilities. Figure 1 shows the relationship of objects in an information security incident.



NOTE The shaded objects are pre-existing, affected by the unshaded objects that result in an information security incident.

Figure 1 — Relationship of objects in an information security incident

Coordination is an important aspect in information security incident management. Many incidents cross organizational boundaries and cannot be easily resolved by a single organization or, a part of an organization where the incident has been detected. Organizations should commit to the overall incident management objectives. Incident management coordination is required across the incident management process for multiple organizations to work together to handle information security incidents. This is for example the role of CERTs and CSIRTs. Information sharing is necessary for incident management coordination, where different organizations share threat, attack, and vulnerability information with each other so that each organization's knowledge benefits the other. Organizations should protect sensitive information during information sharing and communication. See ISO/IEC 27010 for further details.

It is important to indicate that resolving an information security incident should be done within a defined time frame to avoid unacceptable damage or a resulting catastrophe. This resolution delay is not as important in case of an event, vulnerability or a non-conformity.

4.2 Objectives of incident management

As a key part of an organization's overall information security strategy, the organization should put controls including procedures in place to enable a structured well-planned approach to the management of information security incidents. From an organization's perspective, the prime objective is to avoid or contain the impacts of information security incidents in order to minimize the direct and indirect damage to its operations caused by the incidents. Since damage to information assets can have a negative consequence on operations, business and operational perspectives should have a major influence in determining more specific objectives for information security incident management.

More specific objectives of a structured well-planned approach to incident management should include the following:

a) information security events are detected and efficiently dealt with, in particular deciding whether they should be classified as information security incidents;

b) identified information security incidents are assessed and responded to in the most appropriate and efficient manner and within the predetermined time frame;

c) the adverse impact(s) of information security incidents on the organization and involved parties and their operations are minimized by appropriate controls as part of incident response;

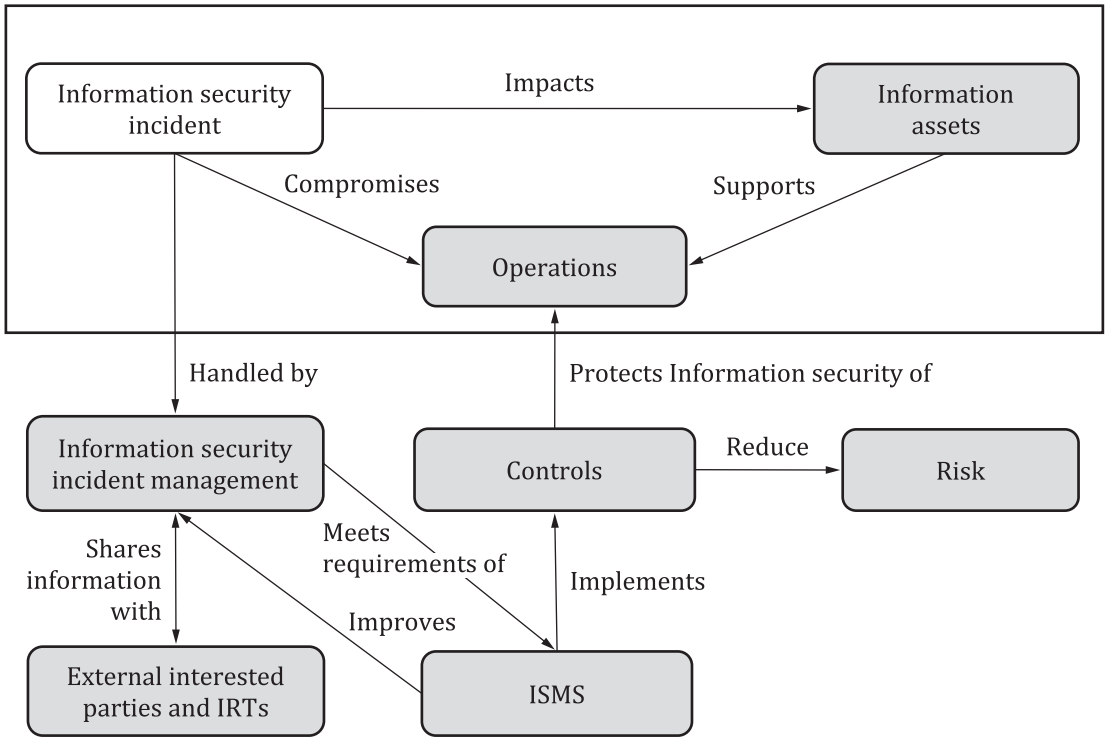
d) a link with relevant elements from crisis management and business continuity management through an escalation process is established. There is a need for a swift transfer of responsibility and action from incident management to crisis management when the situation requires it, with this order reversed once the crisis is resolved to allow for a complete resolution of the incident;

e) information security vulnerabilities involved with or discovered during the incident are assessed and dealt with appropriately to prevent or reduce incidents. This assessment can be done either by the incident response team (IRT) or other teams within the organization and involved parties, depending on duty distribution;

f) lessons are learnt quickly from information security incidents, related vulnerabilities and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.

To help achieve these objectives, organizations should ensure that information security incidents are documented in a consistent manner, using appropriate standards or procedures for incident categorization, classification, prioritization and sharing, so that metrics can be derived from aggregated data over a period of time. This provides valuable information to aid the strategic decision making process when investing in information security controls. The information security incident management system should be able to share information with relevant internal and external parties.

Another objective associated with this document is to provide guidance to organizations that aim to meet the information security management system (ISMS) requirements specified in ISO/IEC 27001 which are supported by guidance from ISO/IEC 27002. ISO/IEC 27001 includes requirements related to information security incident management. Table C.1 provides cross-references on information security incident management clauses from ISO/IEC 27001 and clauses in this document. ISMS relationships are also explained in Figure 2. This document can also support the requirements of information security management systems that do not follow ISO/IEC 27001.



NOTE See also Figure 1.

Figure 2 — Information security incident management in relation to ISMS and applied controls

4.3 Benefits of a structured approach

Using a structured approach to information security incident management can yield significant benefits, which can be grouped under the following topics.

a) Improving overall information security

To ensure adequate identification of and response to information security events and incidents, it is a prerequisite that there be a structured process for planning and preparation, detection, reporting and assessment, and relevant decision-making. This improves overall security by helping to quickly identify and implement a consistent solution, and thus provides a means of preventing similar information security incidents in the future. Furthermore, benefits are gained by metrics, sharing and aggregation. The credibility of the organization can be improved by the demonstration of its implementation of best practices with respect to information security incident management.

b) Reducing adverse business consequences

A structured approach to information security incident management can assist in reducing the level of potential adverse business consequences associated with information security incidents. These consequences can include immediate financial loss and longer-term loss arising from damaged reputation and credibility. For further guidance on consequence assessment, see ISO/IEC 27005. For guidance on information and communication technology readiness for business continuity, see ISO/IEC 27031.

c) Strengthening the focus on information security incident prevention

Using a structured approach to information security incident management helps to create a better focus on incident prevention within an organization, including the development of methods to identify new threats and vulnerabilities. Analysis of incident-related data enables the identification of patterns and trends, thereby facilitating a more accurate focus on incident prevention and identification of appropriate actions and controls to prevent further occurrence.

d) Improving prioritization

A structured approach to information security incident management provides a solid basis for prioritization when conducting information security incident investigations, including the use of effective categorization and classification scales. If there are no clear procedures, there is a risk that investigation activities may be conducted in an overly reactive mode, responding to incidents as they occur and overlooking what activities should be handled with a higher priority.

e) Supporting evidence collection and investigation

If and when needed, clear incident investigation procedures help to ensure that data collection and handling are evidentially sound and legally admissible. These are important considerations if legal prosecution or disciplinary action follows. For more information on digital evidence and investigation, see the investigative standards in Annex A.

f) Contributing to budget and resource justifications

A well-defined and structured approach to information security incident management helps to justify and simplify the allocation of budgets and resources for involved organizational units. Furthermore, benefit accrues for the information security incident management plan itself, with the ability to better plan for the allocation of staff and resources.

One example of a way to control and optimize budget and resources is to add time tracking to information security incident management tasks to facilitate quantitative assessment of the organization's handling of information security incidents. It can provide information on how long it takes to resolve information security incidents of different priorities and on different platforms. If there are bottlenecks in the information security incident management process, these should also be identifiable.

g) Improving updates to information security risk assessment and treatment results

The use of a structured approach to information security incident management facilitates:

— better collection of data for assisting in the identification and determination of the characteristics of the various threat types and associated vulnerabilities, and

— provision of data about frequencies of occurrence of the identified threat types, to assist with analysis of control efficacy (i.e. identify controls that failed and resulted in a breach, with uplift of such controls to reduce reoccurrence).

The data collected about adverse impacts on business operations from information security incidents is useful in business impact analysis. The data collected to identify the frequency of various threat types can improve the quality of a threat assessment. Similarly, the data collected on vulnerabilities can improve the quality of future vulnerability assessments. For guidance on information security risk assessment and treatment, see ISO/IEC 27005.

h) Providing enhanced information security awareness and training programme material

A structured approach to information security incident management enables an organization to collect experience and knowledge of how the organization and involved parties handle incidents, which is valuable material for an information security awareness programme. An awareness programme that includes lessons learned from real experience helps to reduce mistakes or confusion in future information security incident handling and improve potential response times and general awareness of reporting obligations.

i) Providing input to the information security policy and related documentation reviews

Data provided by the practice of a structured approach to information security incident management can offer valuable input to reviews of the effectiveness and subsequent improvement of incident management policies (and other related information security documents). This applies to topic-specific policies and other documents applicable both for organization-wide and for individual systems, services and networks.

4.4 Adaptability

The guidance provided by the ISO/IEC 27035 series is extensive and, if adopted in full, can require significant resources to operate and manage. It is therefore important that an organization applying this guidance should retain a sense of perspective and ensure that the resources applied to information security incident management and the complexity of the mechanisms implemented are proportional to the following:

a) size, structure and business nature of an organization including key critical assets, processes, and data that should be protected;

b) scope of any information security management system for incident handling;

c) potential risk due to incidents;

d) the goals of the business.

An organization using this document should therefore adopt its guidance in a manner that is relevant to the scale and characteristics of its business.

4.5 Capability

4.5.1 General

Information security incidents can jeopardize achievement of business objectives and generate crises. Following the risk assessment, it is possible to delineate between situations whose likelihood is medium to high, and consequence low to medium, and those whose likelihood is (very) rare and consequences very high. The second situation represents crises that are not always possible to completely prevent

and, in some cases, disrupts the decision chain. ISO/IEC 27031 provides guidance on information communication technology (ICT) readiness for business continuity to support business operations in the event of emerging information security events and incidents, and related disruptions.

The overarching objectives of crisis management are:

— to protect human life including critical infrastructure to the extent necessary;

— to support continuity of everyday activity;

— to protect assets including property and the natural environment, as far as possible.

No two crises are the same. These objectives are underpinned by the following principles:

— Coordination: effective coordination and communication facilitates information sharing.

— Continuity: prevention, preparedness, response and recovery to crises should be grounded in the existing functions of organisations and familiar ways of working.

— Proportionality: crisis management should be calibrated to the magnitude and nature of the crisis.

— Accountability: decision-making and actions are transparent and accountable.

— Integration: prevention, preparedness, response and recovery should be considered as elements of a continuum that may occur concurrently.

Information security incident management requires a capability to ensure coherency of management to achieve efficient and effective incident handling. This capability should be established by incident management policy, plan, process and procedure, as well as properly structured team, skilled people, information sharing and coordination with other parties both internal and external.

4.5.2 Policies, plan and process

The organization's policies for information security management should consider how information security incident management aligns with risk management. To achieve this, the organization should identify, as part of the risk management process, the list of events/incidents they want to counter and control, with ensuring as minimal impact as possible on the business operations and objectives.

Incident management requires a defined process approved by the top management that includes flows of actions (or procedures) to be performed at all phases of the process and a communication protocol with appropriate channels.

4.5.3 Incident management structure

To allow a coherent response to the events and incidents, organizations should institute an incident management capability that prepares the information security incident management policy and describes the incident response structure. Organizations should also ensure that the directives and resources exist to adequately respond to the incidents.

a) Incident management team

An incident management team (IMT) consists of appropriately skilled and trusted members of an organization with the role of leading all information security incident management activities, in coordination with other parties, both internal and external, throughout the incident life cycle. IMT provides all necessary services to cope with incidents, not only preparing for, detecting, reporting, assessing, and responding to incidents, but also threat and vulnerability detection, advisory, information sharing, learning lessons, improvement, education and awareness. IMT can introduce any necessary resources at any time in order to provide these services.

The organization should determine and allocate roles and responsibilities to handle, coordinate and respond to the incidents. This includes:

b) Point of contact

The point of contact (PoC) is the role, address or person which personnel can turn to when they discover anomalies and what is considered as an event in the policy and awareness sessions. Depending on the nature and size of the organizations, there can be more than one PoC. For example, one for ICT issues and one for physical, organizational and procedural situations, which is similar to what already exists for accidents, fire and other damaged equipment.

c) Incident coordinator who:

— coordinates and manages event notifications and alerts that are raised either by information systems or individuals,

— performs the evaluation of the event and declares the incident,

— activates the IRT(s) and coordinates its/their activities,

— records all information on the incident and its resolution,

— completes and sends the incident report, with their proposals for improvement,

— coordinates with internal and external organisations following the IMT's direction with respect of incident handling.

NOTE The organization can decide to use another term for the incident coordinator.

The incident coordinator allocated should maintain control for the whole duration of the incident. Where an incident goes beyond the work shift and requires someone to remain present/available, another incident coordinator should take over with all the necessary information and authority.

If a call to the BCP (business continuity planning)/DRP (disaster recovery planning) coordinator or team is required, the incident coordinator should remain informed, and resume managing the incident upon crisis resolution, as to complete resolution.

d) Incident response teams (IRTs) that:

— perform the "procedures" to respond to the incident,

— detect the root cause(s) and hidden vulnerabilities,

— resolve the incident,

— report to the incident coordinator.

e) Change management team that decides on the actions to be taken to improve the incident prevention and response.

f) Awareness and training team that prepares the programme and sessions aimed to identify and report unwanted events.

g) Vulnerability management team that analyses the vulnerabilities detected during the incident response and provides its recommendations to the change management team.

h) Crisis management team that ensures the coordination with the BCP/DRP coordinator or team

i) Security monitoring team that updates the monitoring and detection system rules in application of a decision following lessons learned, and monitors for reoccurrence of similar incidents.

4.6 Communication

Organizations should communicate the approved information security incident management policies to interested parties. This includes both internal staff and external parties with access to the organization's information. The organization should communicate the following:

— the organization's information security incident policies and relevant procedures;

— obligations/expectations of personnel;

— incident reporting procedures;

— who to contact for more information;

— outcomes of incidents and how to minimize reoccurrence.

The organization should promote incident management as a "no-fault" reporting process to empower personnel to come forward and report incidents without the fear of retribution. Focus should instead be on the positive outcomes that an organization can gain from receiving incident reporting, learning and improving from incidents to become more secure and resilient.

Reporting of incidents is "no-fault" in the first instance i.e. no fault or blame will be associated with a reported incident. Following investigation, sanctions may occur if the incident is found to be the result of intentional violation of the organization's policies and procedures, or in repeated instances of misconduct or negligence.

Communication is essential to control the messaging surrounding the incident including where, when, what and how this messaging is delivered, both to provide the appropriate response and to satisfy organizational or societal needs. Internal communication is necessary for an effective response and recovery, and external communication is indispensable e.g. for company image.

NOTE An information breach (aka uncontrolled communication) about an incident can have serious consequences.

Only duly mandated and prepared personnel should be allowed to communicate with the external world as to only tell what is necessary, at the best moment and in the appropriate form.

4.7 Documentation

4.7.1 General

It is crucial to document as much information as possible related to the event/incident from its detection through to its resolution. The incident report is the synthesis of all this information.

4.7.2 Event report

The event report should contain all that is necessary to understand the event and make a decision regarding whether to classify the event as an incident. This includes:

a) date and time of the detection;

b) name of informant which can however be hidden to keep confidentiality;

c) all circumstances and facts for comprehension of the event.

4.7.3 Incident management log

All information gathered during the incident response should be documented/recorded/logged to serve as a record of actions i.e. date/time and corresponding action/decision.

4.7.4 Incident report

The incident report is the synthesis of all gathered information throughout the incident life cycle. It serves to analyse and evaluate the incident, and decide if changes are planned for incident management capability (see also 4.5).

A pre-formatted template document for incident reports should be prepared to ensure no essential information is missed or overlooked.

4.7.5 Incident register

All information security incidents should be recorded in a centrally managed incident register. This register provides the IMT with an overview of the incidents that have occurred in the organization, their status, and any follow up activities. It can also be used by the IMT to provide reports to top management regarding trends and themes around the threat environment and feed into organizational planning and risk assessments.

5 Process

5.1 Overview

To achieve the objectives outlined in 4.2, information security incident management process consists of five distinct phases:

— plan and prepare (see 5.2);

— detect and report (see 5.3);

— assess and decide (see 5.4);

— respond (see 5.5);

— learn lessons (see 5.6).

A high-level view of these phases is shown in Figure 3.

Some activities can occur in multiple phases or throughout the incident handling process. Such activities include the following:

— documentation of event and incident evidence and key information, response actions taken, and follow-up actions done as part of the incident handling process;

— coordination and communication between the involved parties;

— notification of significant incidents to management and other interested parties;

— information sharing between interested parties and internal and external collaborators such as vendors and other IRTs.

The time considerations for each step in the event/incident management process should be:

a) Detection: as soon as possible

b) Reporting: complete required forms without unnecessary delay, or via automated methods.

c) Response: as soon as possible to start the response before the damages (impacts and consequences) exceed the organizationally-determined limits to avoid having a situation that requires taking BCP/DRP measures. Acceptable limits should be well defined in BCP and known by everyone. Each type of incident may therefore have a different path for or mode of resolution.

d) Communication

   — Internal: to adopt, as soon as possible, measures and behaviours and prevent prolonging of the incident

   — External: to receive, as soon as possible, the necessary help from relevant external intervening parties, and notify the interested parties

e) Escalation: within an organizationally-determined interval and/or before impacts exceed organizationally-determined limits

f) Notification: within an organizationally-determined interval or any legally required interval.

All actions should be performed and monitored with no unnecessary delay.

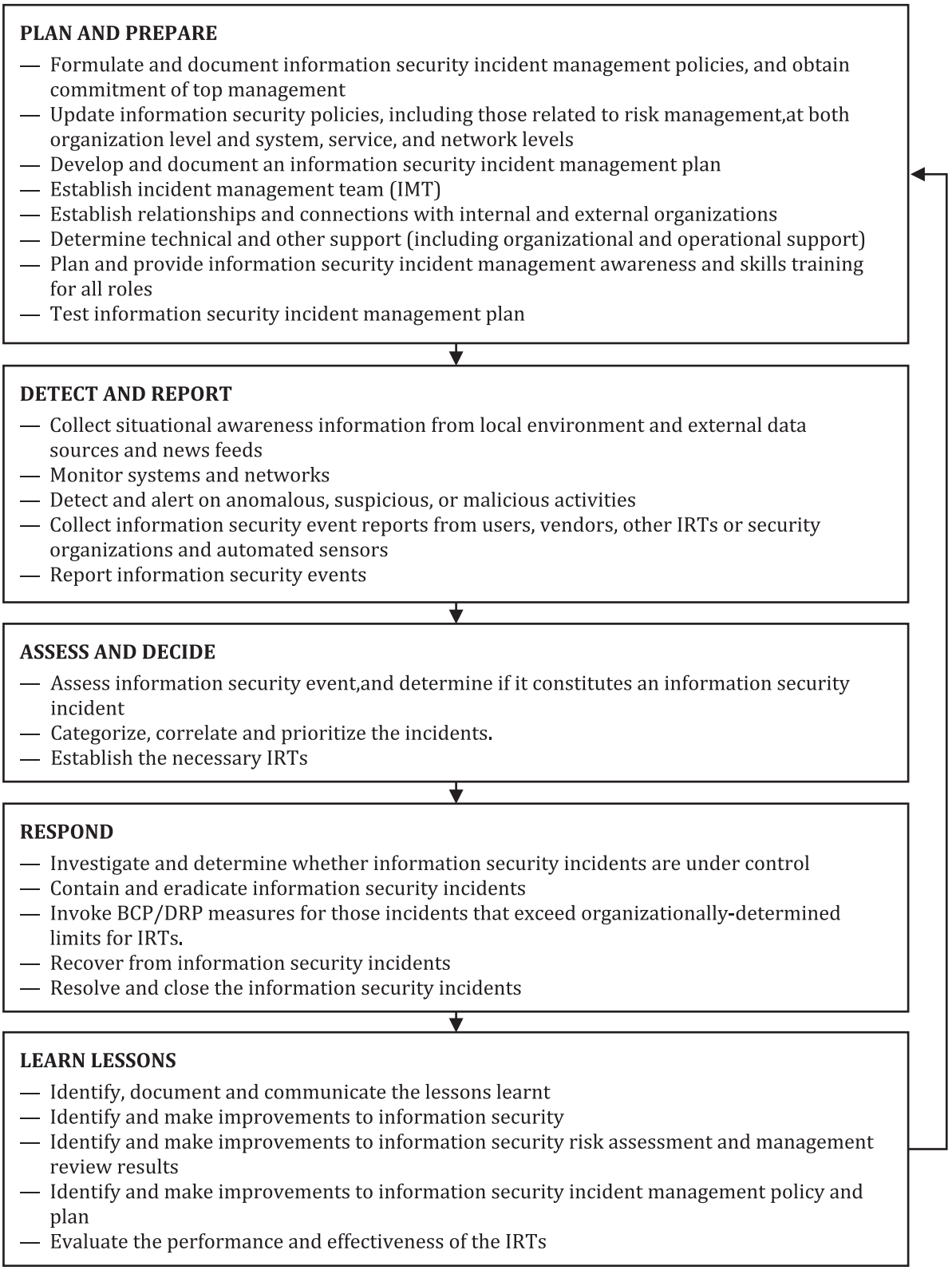


Figure 3 — Information security incident management phases

Figure 4 shows the flow of information security events and incidents through information security incident management phases and related activities.

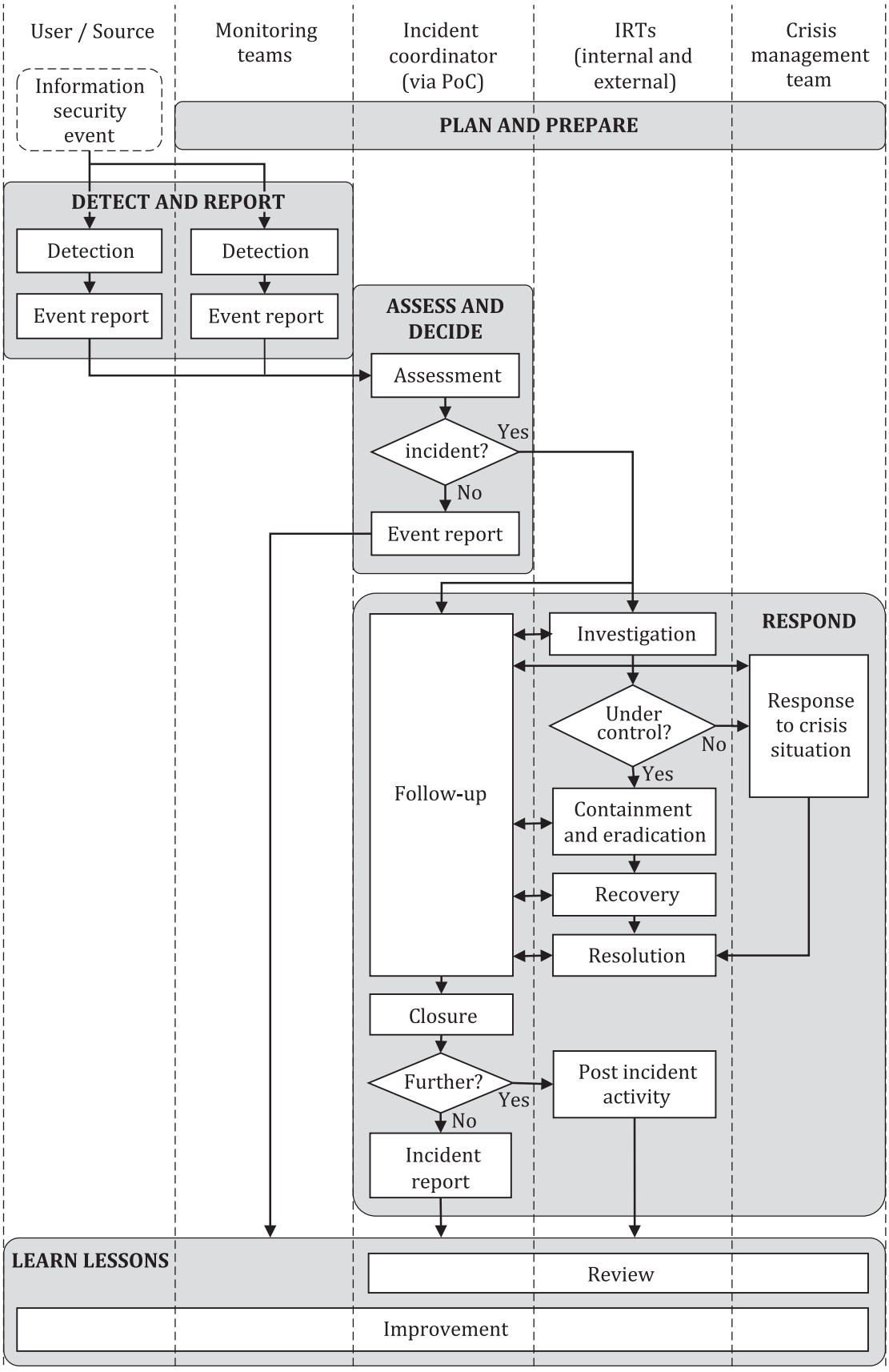


Figure 4 — Information security event and incident flow diagram

5.2 Plan and prepare

Effective information security incident management requires appropriate planning and preparation. It is essential to keep calm at all stages of incident response, and that this response time is controlled and mastered. If it is not, prolonged incident duration may increase adverse impact to the organization. This response time should be computed as a portion of the recovery time objective (RTO, see ISO/IEC 27031:2011, 3.13 and 6.3) and should take into consideration the inevitable delay necessary for detection, reporting and assessment.

For an efficient and effective information security incident management plan to be put into operation, an organization should complete a number of preparatory activities in support of the incident management requirements of ISMS, namely:

a) formulate and document information security incident management policies and obtain commitment of top management, including purpose, objectives and scope of policies, categories and criteria for determining and prioritizing incidents, organizational structure and setting of roles, responsibilities and authorities for incident management, performance measures, reporting and contact forms;

b) update information security policies, including those related to risk management, at both organization level and system, service or network level;

c) develop and document a detailed information security incident management plan, including procedures and methods for incident handling, communications and information sharing, by which to establish incident management capability. The organization should

   — define information security event/incident indicators and precursors;

   — list possible events/incidents that the organization wants to be able to control. This list is mainly based on the result of the risk assessment. An event/incident is a risk that becomes real;

   — formulate the format and content of the incident report. This enables consistent reporting regardless of the individual filling in the form and is important for lessons learned as well as determining common themes and trends for reporting up to management;

   — define/establish incident categories;

   — establish handover procedures for handover to law enforcement when administrative incidents (e.g. policy violation) become criminal incidents (e.g. fraud);

   — document the evaluation procedure to declare an incident;

   — determine the information and responsibility exchange with the crisis management team (BCP/DRP) in both directions;

   — establish an incident management team that gathers all the skills necessary to prepare the incident response plan;

   — establish a decision/command structure and an emergency call tree;

   — provide essential internal and external contact points (e.g. legal);

   — set up an incident response team(s) (IRT) whose role is to respond to and resolve the incident. Several IRTs can exist with specific skills to respond to specific incidents. More information can be found in ISO/IEC 27035-2:2023, 7.3.

d) determine the IRT, with its functions and services, and an appropriate training programme designed, developed, and provided to its personnel. The response teams should know what to do, which resources to use and in which time frames. It is essential that the personnel is trained to perform with efficiency and ability to work under pressure.

e) establish and preserve appropriate relationships and connections with internal and external organizations that are directly involved in information security event, incident, threat and vulnerability management, and communicate information security incident management policies and procedures to them;

f) establish, implement and operate technical, organizational and operational mechanisms to support the information security incident management plan. Develop and deploy necessary information systems to support the incident response, including an information security incident register. These mechanisms and systems are intended to prevent information security incident occurrences or reduce the likelihood of occurrences of information security incidents;

g) design and develop an awareness and training programme for information security event, incident and vulnerability management;

h) test the use of the information security incident management plan, its processes and procedures.

With this phase completed, organizations should be fully prepared to properly manage information security incidents. ISO/IEC 27035-2:2023, Clauses 4 to 11, describes each of the activities listed above, including the contents of policy and planning documents.

5.3 Detect and report

The second phase of information security incident management involves the detection of, collection of information associated with, and reporting on, occurrences of information security events and the discovered or involved information security vulnerabilities, by manual or automatic means. In this phase, events and vulnerabilities cannot yet be classified as information security incidents.

It is likely that several channels exist for reporting security events to the adequate point of contact (PoC) using the event report. While some ICT and technical events are reported to an ICT department, other issues, such as privacy breaches, may be raised to other departments of the organization. The organization should have procedures in place to distribute the event reports to the incident coordinator to enable coordination and overview of all information security incidents. The incident coordinator should coordinate these different inputs with other departments of the business. Police, ambulances, fire brigades and other emergency services are sometimes reached at different telephone numbers. Further, the communication channels can be different: telephone, fax, beeper, email, automated alarm in ICT systems, mobile push notification, (operator's) dashboard, etc.

The entity that detects the situation is not always the one that suffers from its consequences (e.g. a security agent detecting an intrusion and a theft in offices, a fire in a house detected by a neighbour). It is important to consider the concept of targeted or impacted business team/entity, which is the business activity and more exactly the personnel/entity who performs it and its related management.

The reporting of security events in line with the organization's reporting policies enables later analysis if required.

For the detect and report phase, an organization should undertake the following key activities:

a) monitor by monitoring systems or monitoring teams (e.g. watching for camera images) and log system and network activity as appropriate;

b) detect and report the occurrence of an information security event or the existence of related vulnerabilities and threats, whether manually by personnel or automatically;

c) collect information on an information security event or related vulnerabilities and threats;

d) collect situational awareness information from internal and external data sources including local system and network traffic and activity logs, news feeds concerning ongoing political, social, or economic activities that can impact incident activity, external feeds on incident trends, new attack vectors, indicators of compromise and new mitigation strategies and technologies;

e) perform external/internal threat analysis to establish an understanding of the threat environment and in turn detect changes;

f) determine and include the reliability and quality of the information being analysed of the threat assessments;

g) perform regular analysis for vulnerabilities and attack vectors, based on the existing and potential threats;

h) ensure that all detection activities and results are properly logged for later analysis;

i) ensure that digital evidence is gathered and stored securely, and that its secure preservation is continually monitored, in case the evidence is required for legal prosecution or internal disciplinary action. For more detailed information on the identification, collection, acquisition and preservation of digital evidence, see the investigative standards listed in Annex A;

j) inform, on an as-needed basis throughout the phase, for further review or decisions.

All information collected pertaining to an information security event or related vulnerabilities and threats should be stored in the information security incident register managed by the IMT. The information reported during each activity should be as complete as possible at the time. This supports assessments, decisions and actions to be taken.

5.4 Assess and decide

The third phase of information security incident management involves the assessment of information associated with occurrences of information security events and the decision on whether to classify events as information security incidents. The incident coordinator evaluates the event based on the event report and the criteria defined during the plan and prepare phase and declare if it is an incident or not.

Once an information security event has been detected and reported, the subsequent activities should be performed.

a) Distribute the responsibility for information security incident management activities through an appropriate hierarchy of personnel with assessment, decision making and actions involving both security and non-security personnel.

b) Provide formal procedures for each notified person to follow, including reviewing and amending reports, assessing damage, and notifying relevant personnel. Individual actions depend on the type and severity of the incident.

c) Use guidelines for thorough documentation of an information security event and the subsequent actions for an information security incident if the information security event becomes classified as an information security incident.

d) Evaluate whether the event is an incident or not, correlate the event for reoccurrence and retrieve data from prior actions and responses. The type and time frame for resolution depends on this decision based on factors decided during the plan and prepare phase. The decision criteria should be clear and tested, considering technological, business and human aspects. Prioritize all information security incidents according to relevant internal documentation.

e) Communicate through the established and already activated channels and protocols to the IRT(s) and to business management, when needed.

f) Call to the response team(s) necessary to respond and resolve the various problems identified during detection and the information provided by the finder/reporter.

g) Gather information of the targeted or affected teams.

h) Start the timer for the response.

It is crucial that a decision to declare an event as an information security incident is made rapidly as it allows the rapid designation of the IRT and setting the "count-down" process to make sure the incident is resolved within the expected time frame. Decision tables should have been prepared during the plan and prepare phase.

For the assess and decide phase, an organization should perform the following key activities:

i) Collect information that can include testing, measuring, and other data gathering about the detection of an information security event. The type and amount of information collected will depend on the information security event that has occurred.

j) Conduct an assessment by the incident coordinator to determine whether the event is a possible or confirmed information security incident or a false alarm. A false alarm (i.e. a false positive) is an indication of a reported event that is found not to be real or of any impact. If desired, the IRT can conduct a quality review to ensure that the incident coordinator correctly declared an incident.

k) Log all activities, results and related decisions for later analysis and recordkeeping.

l) Ensure that the change control regime is maintained to cover information security incident tracking and incident report updates, and to keep the information security incident register up to date.

All information collected pertaining to an information security event/incident or related vulnerabilities and threats should be stored in the information security incident register managed by the IMT. The information reported during each activity should be as complete as possible at the time. This supports assessments, decisions and actions to be taken.

5.5 Respond

The fourth phase of information security incident management involves responding to information security incidents in accordance with the decision in the assess and decide phase, and the procedures described in the response plan elaborated during the plan and prepare phase. Depending on the decisions, the responses can be made immediately, in real-time, or in near real-time, and some responses can involve information security investigation. The incident coordinator is the key role to coordinate the activities of the IRT(s) and monitor the response timer.

Each type of incident will receive its specific response. Depending on what is discovered by the IRT(s) during activation, the incident response may take various/different paths to recovery and may require varying/differing resources.

The information security incident coordinator is kept up to date at a frequency commensurate with incident severity, and may make decisions to contact other teams with specific skills depending on the need to respond to the discovered incident or repair/restore the defective, damaged or destroyed assets (physical, material, software, procedural, organizational, etc.).

When responding to an event rather than an incident, generally, an event is solved within the normal business processes, as there is no emergency or immediate danger.

The incident coordinator keeps regular contact with the targeted/affected teams/entities of the incident and decides, with them, if the incident is resolved or not. It is to further ensure if sufficient resources are available to start business activities again. The situation can however require a more complete resolution, with complete restoration and resumption of capabilities and operations.

The incident coordinator prepares the incident report which should include:

— analysis of the situation;

— identification of the problem and, if possible, its cause;

— determination of the gravity/seriousness and the urgency to respond;

— inclusion in the change programme.

NOTE 1 If the incident resolution exceeds the work shift of the incident coordinator (e.g. more than 8 hours to several days), the initial incident coordinator gathers all received information and notes taken by all involved incident coordinator(s) as to produce the final report. He/she remains the main incident coordinator.

The response procedure to be followed requires:

— a clear definition of the incident to be managed and controlled;

— a list of necessary and required resources;

— a detailed chronology of the actions to be performed, with timing;

— the target resolution time frame;

— a list of contact points and channels for information with the criteria;

— the skills and size of the teams (with the necessary/required training);

— the presence of the resources.

Once an information security incident has been confirmed and the responses determined, the subsequent activities should be undertaken:

a) Distribute the responsibility for information security incident management activities through an appropriate hierarchy of personnel with decision making and actions, involving both security and non-security personnel as necessary.

b) Provide formal procedures for each involved person to follow, including reviewing and amending the reports, reassessing damage, and notifying the relevant personnel. Individual actions depend on the type and severity of the incident. For more information on ICT incident response, see ISO/IEC 27035-3:2020, Clauses 8, 9 and 11.

c) Reconsider the original assessment as additional information becomes available to identify whether the information security incident shall be re-prioritised, or response activities adjusted.

d) Use guidelines for thorough documentation of an information security incident and subsequent actions.

e) Evaluate the proposed resolution with targeted/affected teams/entities to ensure it meets the resolution criteria and expectations of all parties involved.

f) Investigate incidents as required and relative to the information security incident classification scale rating. The rating should be changed as necessary. Investigation can include different kinds of analyses to provide a more in-depth understanding of incidents.

g) Review by the incident coordinator and IRT to determine whether the information security incident is under control, and if so, perform the required response. If the incident is not under control, or will result in severe adverse impact to the organization, escalate it to the crisis management team. Escalation can result in action (response) at two different levels:

   — one that falls within the responsibility and authority of the incident coordinator (see 5.2 and 5.3) to, for example, call more response teams with different skills to cope with what is discovered (it is what happens in case of a fire when the emergency point of contact calls ambulances, police and other fire-fighter teams);

   — one that falls beyond the authority of the incident coordinator who then calls for another management level (e.g. involvement of another department in the organization, call for external support with financial consequences that requires the authorization by the finance department).

h) Assign internal resources and identify external resources in order to respond to an incident.

i) Ensure that all parties involved, particularly the IRT, properly log all activities for later analysis.

j) Ensure that digital evidence is gathered and stored provably securely, and that its secure preservation is continually monitored, in case the evidence is required for legal prosecution or internal disciplinary action.

Gathering digital evidence includes the following actions:

— provide frequent status updates to key stakeholders;

— gather, record, and maintain a chain of custody of evidence related to the incident;

— notify regulators of the incident (where applicable);

— update the incident register with incident closure details;

— follow any retention and preservation of evidence relating to the information security incident (legal and regulatory requirements can apply).

NOTE 2 For more detailed information on the identification, collection, acquisition and preservation of digital evidence, see the investigative standards listed in Annex A.

k) Ensure that the change control regime is maintained to cover information security incident tracking and incident report updates, and to keep the information security incident register up to date.

l) Follow pre-defined communication protocols and/or an engagement plan that identifies who has the authority to communicate to different stakeholders, and communicate the existence of the information security incident and share any relevant details (e.g. threat, attack, and vulnerability information) with other internal and external individuals or organizations, in accordance with organizational and incident management communication plans and information disclosure policies. It can be particularly important to notify asset owners (determined during the impact analysis) and internal and external organizations (e.g. other incident response teams, law enforcement agencies, Internet service providers, and information sharing organizations) that can assist with the management and resolution of the incident. Sharing information can also benefit other organizations since the same threats and attacks often affect multiple organizations. For further detail about information sharing, see ISO/IEC 27010.

m) After recovery from an incident, a post incident activity should be initiated depending on the nature and severity of the incident. This activity includes:

— investigation of the information pertaining to the incident,

— investigation of other relevant sources such as involved personnel,

— summarized report of the investigation findings.

n) Once the incident has been resolved, it should be closed according to the rules defined in the information security incident management policy and all interested parties should be notified.

All information collected pertaining to an information security event/incident, or related vulnerabilities and threats should be stored in the information security incident register managed by the IMT. The information reported during each activity should be as complete as possible at the time. This supports assessments, decisions and actions to be taken, including potential further analysis.

5.6 Learn lessons

The fifth phase of information security incident management occurs when information security incidents have been resolved. This phase involves learning lessons from how incidents, related vulnerabilities and threats have been handled.

Lessons can come from one or many information security incidents or reported security vulnerabilities. Improvements are aided by metrics fed into the organization's strategy on where to invest in information security controls. It is crucial that lessons learned are linked with the information security management change capability that makes the business decisions and, when deemed necessary, include the proposed modification in the information security management improvement process.

The incident report should indicate various situations leading to different actions to be forwarded to the information security management improvement process. The report should also make improvements to the information security incident management plan and its documentation based on the lessons learned.

For the learn lessons phase, an organization should perform the following key activities:

a) review how effective the processes, procedures, reporting formats and organizational structure were in responding to, assessing and recovering from information security incidents and dealing with information security vulnerabilities;

b) identify, document and communicate the lessons learned from information security incidents, related vulnerabilities and threats;

c) review, identify and make improvements to information security control implementation (new or updated controls), as well as information security incident management policy;

d) review, identify and make improvements to the organization's existing information security risk assessment and management reviews;

e) communicate and share the results of review within a trusted community (if the organization so wishes);

f) determine if the incident information, associated attack vectors and vulnerabilities may be shared with partner organizations to assist in preventing the same incidents from occurring in their environments. For more details, see ISO/IEC 27010 on information sharing;

g) perform a comprehensive evaluation of IRT performance and effectiveness on a periodic basis.

It is emphasized that information security incident management activities are iterative, and therefore an organization should make regular improvements to a number of information security elements over time. These improvements should be proposed on the basis of reviews of the data on information security incidents, responses, and reported information security vulnerabilities.

Annex D provides considerations of situations discovered during the investigation of an incident.

ISO/IEC 27035-2:2023, Clause 12 describes in detail each of the activities listed above.

Annex A
(informative)

Relationship to investigative standards

This document describes part of a comprehensive investigative process which includes, but is not limited to, the application of the following standards:

— ISO/IEC 27037

ISO/IEC 27037 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

Some documents can contain information that should 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 shall not 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 should not be recoverable. Hence, care shall be taken so that redacted information is permanently removed from the digital document (e.g. it should 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

ISO/IEC 27040 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 should 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. ISO/IEC 27041 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 document 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

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

— the ISO/IEC 27050 series

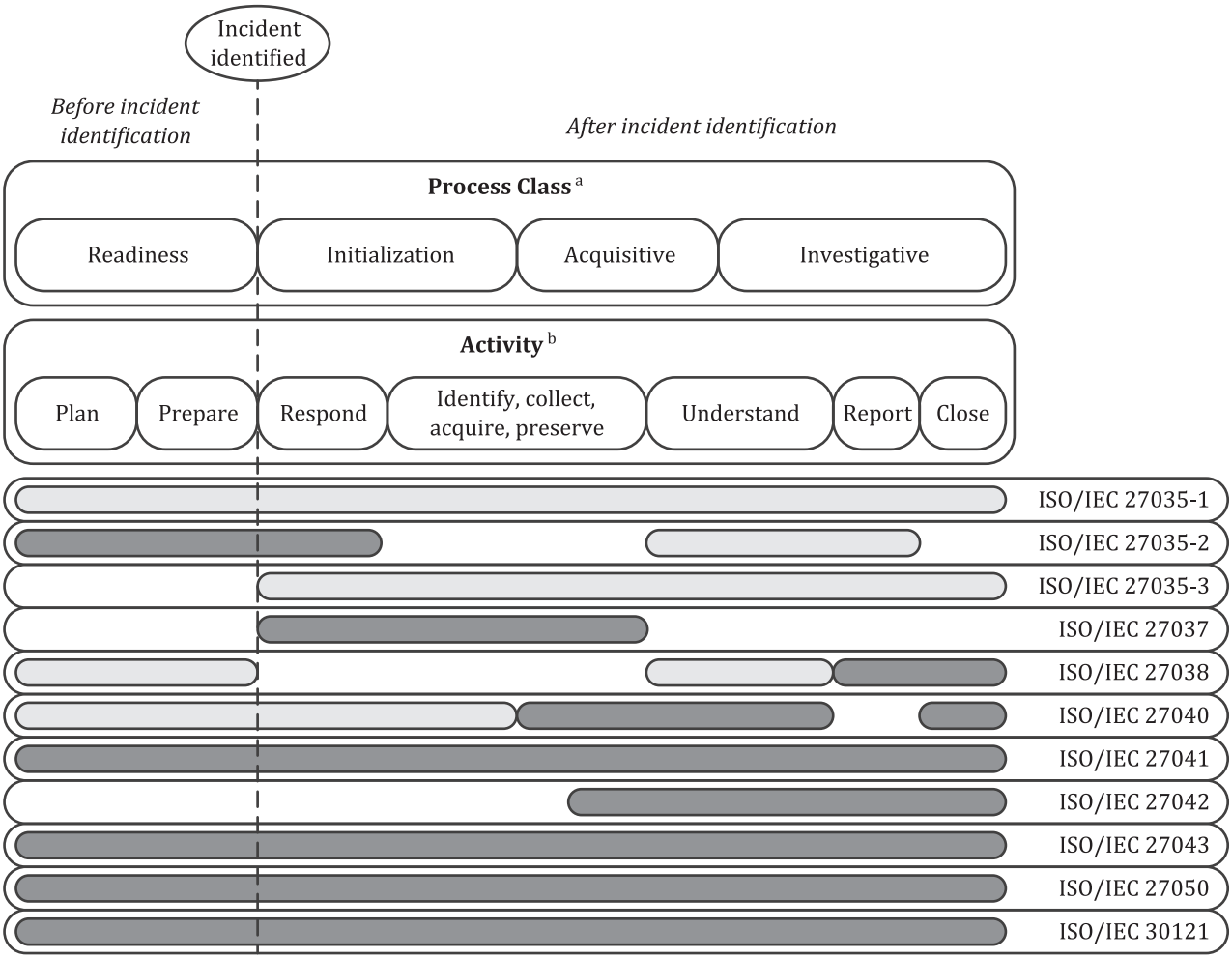
The ISO/IEC 27050 series addresses activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of Electronically Stored Information (ESI). In addition, it provides guidance on measures, spanning from initial 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.

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

ISO/IEC 30121 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. ISO/IEC 30121 applies to the development of strategic processes (and decisions) relating to the retention, availability, access and cost effectiveness of digital evidence disclosure. ISO/IEC 30121 is applicable to all types and sizes of organizations. ISO/IEC 30121 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 can occur as the result of inevitable security breaches, fraud, and reputation assertion. In every situation Information Technology (IT) should be strategically deployed to maximize the effectiveness of evidential availability, accessibility and cost efficiency

Figure A.1 shows typical activities surrounding an incident and its investigation. The document reference numbers shown in this figure (e.g. ISO/IEC 27037) indicate the documents 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 of the documents are consulted prior to, and during, the planning and preparation phases. The process classes shown are defined fully in ISO/IEC 27043 and the activities identified match those discussed in more detail in ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27042 and ISO/IEC 27041.



Key

the document can be directly applied to these activities

the document contains information which may influence and/or assist with these activities

a Process classes are defined in ISO/IEC 27043.

b Detail of activities is given in ISO/IEC 27035-2, ISO/IEC 27037, and ISO/IEC 27042.

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

Annex B
(informative)

Examples of information security incidents and their causes

B.1 Type of incidents

B.1.1 General

Events and incidents covered by the ISO/IEC 27035 series concern information and ICT security. Such events and incidents result from imperfect risk management and the continuous advancement of people, processes and technology – and their associated vulnerabilities – in the context of evolving attacker motivation and capability.

The events/incidents happen in the following domains and incident management should cover all potential cases.

B.1.2 Confidentiality

Information leaks may have immediate effects on an organization, and may make information irretrievably available to unauthorized attackers and/or criminals.

One should hence "close the doors" (i.e. stop the leak, fill the breach) and prevent future breaches by identifying the place where it happened and its cause.

B.1.3 Integrity

Integrity incidents (unduly modified information) should be detected and corrected before the information is published and/or used.

Prevention is necessary by identifying the cause.

B.1.4 Availability

Unavailability of information (unreachable, unusable, wiped or disappeared information) can create effects in relation with the service level agreement (SLA) and the RPO. The information should be found and recovered before the business effect is unacceptable.

EXAMPLE A completed financial report ready to be sent to the fiscal authorities at a defined date was not respected.

B.1.5 Access control

Unauthorized access leads to system compromise, theft of resources, and information breach.

Future occurrences should be prevented by identifying underlying exposures and causes and, where applicable, review of access control permissions (authorization, authentication, roles, privileges, network access, etc.)

B.1.6 Vulnerabilities

A technical, people or procedural vulnerability, such as an incorrect allocation of access rights, may allow for successful exploitation. Examples of vulnerabilities include:

— unpatched server, machine or software (not up to date);

— insufficient protection of assets (information, equipment, rooms) with regards to the criticality.

B.1.7 Technical failure

Technical failures render the ICT or physical device inoperative or unusable. It creates either a vulnerability or potential breach of the SLA and the RTO.

B.1.8 Theft or loss of equipment

Theft and loss of equipment, principally those containing information, should be considered as availability and/or confidentiality incidents.

B.2 Attacks

B.2.1 Denial of Service

Denial of Service (DoS) and Distributed Denial of Service (DDoS) are a broad category of incidents with a common thread. Such incidents cause a system, service or network to fail to continue operating in its intended capacity, most often with complete denial of access to legitimate users. There are two main types of DoS/DDoS incidents caused by technical means: resource elimination and resource starvation.

Typical examples of deliberate technical DoS/DDoS incidents include the following:

— forging of traffic (such as pinging) to network broadcast addresses or other services in an effort to overwhelm a target organization's network bandwidth;

— sending data in an unexpected format to a system, service or network in an attempt to crash it, or disrupt its normal operation;

— opening up multiple authorized sessions with a particular system, service or network in an attempt to exhaust its resources (i.e. to slow it down, lock it up or crash it).

Such attacks are often performed through bots, a computer system running malware that is controlled via a botnet. A botnet is a central bot command and control network managed by humans. Botnet sizes can range from hundreds to millions of affected computers.

Some technical DoS incidents can be caused accidentally, for example, caused by operator misconfiguration or through incompatibility of application software, but most of the time, they are deliberate. Some technical DoS incidents are intentionally launched in order to crash a system or service, or take down a network, while others are merely the by-products of other malicious activity. For instance, some of the more common stealth scanning and identification techniques can cause older or misconfigured systems or services to crash when scanned. It should be noted that many deliberate technical DoS incidents are often executed anonymously (i.e. the source of the attack is "faked"), since they typically do not rely on the attacker receiving any information back from the network or system being attacked.

DoS incidents caused by non-technical means, resulting in loss of information, service and/or facilities, can be caused, for example, by:

— breaches of physical security arrangements resulting in theft or wilful damage and destruction of equipment;

— accidental damage to hardware (and/or its location) by fire or water damage/flood;

— extreme environmental conditions, for example high operating temperatures (e.g. due to air conditioning failure);

— system malfunctions or overload;

— uncontrolled system changes;

— malfunctions of software or hardware.

B.2.2 Unauthorized access

In general, this category of incidents consists of actual unauthorized attempts to access or misuse a system, service or network. Some examples of technical unauthorized access incidents include:

— attempts to retrieve password files;

— buffer overflow attacks to attempt to gain privileged (e.g. system administrator) access to a target;

— exploitation of protocol vulnerabilities to hijack or misdirect legitimate network connections;

— attempts to elevate privileges to resources or information beyond what a user or administrator already legitimately possesses;

— compromise at the domain name registrar or hosting provider level, that results in loss of control of the organization's domain portfolio, email service, or of website operations or content.

Unauthorized access incidents caused by non-technical means, resulting in direct or indirect disclosure or modification of information, breaches of accountability or misuse of information systems, can be caused, for example, by:

— breaches of physical security arrangements resulting in unauthorized access to information;

— poorly and/or misconfigured operating systems due to uncontrolled system changes, or malfunctions of software or hardware;

— malicious insider e.g. personnel using their access to the organization’s information assets for personal gain.

B.2.3 Malware

Malware is a program or part of a program inserted into another program with the intent to modify its original behaviour, usually to perform malicious activities such as information and identity theft, information and resource destruction, Denial of Service, spam, etc. Malware attacks can be divided into five categories: viruses, worms, Trojan horses, mobile code and blended. While viruses are created to target any vulnerable infected system, other malware are also used to perform targeted attacks. This is sometimes performed by modifying existing malware and creating a variant that often is not recognized by malware detection technologies.

B.2.4 Abuse

This kind of incident occurs when a user violates an organization's information system security policies. Such incidents are not attacks in the strict sense of the word, but are often reported as incidents and should be handled by an IRT. Inappropriate usage can include:

— downloading and installing hacking tools;

— using corporate e-mail for spam or promotion of personal business;

— using corporate resources to set up an unauthorized website;

— using peer-to-peer activities to acquire or distribute pirated files (music, video, software);

— abusing physical or logical access to steal information for personal gain;

— abusing privilege/position to get information and disclosing it to other parties.

B.3 Information gathering

In general terms, the information gathering category of incidents includes those activities associated with identifying potential targets and understanding the services running on those targets. This type of incident involves reconnaissance, with the goal being to identify:

— the existence of a target, and to understand the network physical or logical topology (e.g. IT network, facility, organisational structure) surrounding it, and with whom the target routinely communicates;

— potential vulnerabilities in the target or its immediate environment that can be exploited.

Typical examples of information gathering by technical means include the following:

— reconnaissance and identification of a victim's online infrastructure by performing searches on known domain names or IP addresses, or by analysing passive DNS information;

— pinging network addresses to find systems that are “alive”;

— probing the system to identify (e.g. fingerprint) the host operating system;

— scanning the available network ports on a system to identify network services [e.g. e-mail, File Transfer Protocol (FTP), web, etc.] and the software versions of those services;

— scanning for one or more known vulnerable services across a network address range (horizontal scanning).

In some cases, technical information gathering extends into unauthorized access if, for example, as part of searching for vulnerabilities, the attacker also attempts to gain unauthorized access. This commonly occurs with automated tools that not only search for vulnerabilities but also automatically attempt to exploit the vulnerable systems, services and/or networks that are found.

Information gathering incidents caused by non-technical means, resulting in:

— direct or indirect disclosure or modification of information;

— theft of intellectual property stored electronically;

— breaches of accountability, e.g. in account logging;

— misuse of information systems (e.g. contrary to law or organization policy).

Information gathering incidents can be caused, for example, by:

— breaches of physical security arrangements resulting in unauthorized access to information, and theft of data storage equipment that contains important data, for example encryption keys;

— poorly and/or misconfigured operating systems due to uncontrolled system changes, or malfunctions of software or hardware, resulting in internal or external personnel gaining access to information for which they have no authority;

— social engineering, which is an act of manipulating people into performing actions or divulging confidential information, e.g. phishing, impersonation of someone else in a phone call;

— tailgating into restricted areas;

— listening in on conversations;

— shoulder surfing/oversight of open documents;

— dumpster diving;

— manipulation of staff.

Annex C
(informative)

Cross-reference table of ISO/IEC 27001 to the ISO/IEC 27035 series

Table C.1 shows references from ISO/IEC 27001:2022, Annex A, regarding information security incident management and where these references correspond in the ISO/IEC 27035 series. The specific subclauses of each document are indicated at the beginning of each row.

Table C.1 — Cross-references from ISO/IEC 27001:2022 in the ISO/IEC 27035 series

ISO/IEC 27001:2022, Annex A	ISO/IEC 27035 series
5.24 Information security incident management planning and preparation Control: The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	**ISO/IEC 27035-1:2023** **5.2 Plan and prepare** **ISO/IEC 27035-2:2023** **4 Information security incident management policy** **5 Updating of information security policies** **6 Creating information security incident management plan** **7 Establishing an incident management capability** **8 Establishing internal and external relationships** **9 Defining technical and other support** **10 Creating information security incident awareness and training** **11 Testing the information security incident management plan**
6.8 Information security event reporting Control: The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	**ISO/IEC 27035-1:2023** **5.3 Detect and report** **ISO/IEC 27035-3:2020** **7 Incident detection operations** **8 Incident notification operations** **12 Incident reporting operations**
5.25 Assessment and decision on information security events Control: The organization shall assess information security events and decide if they are to be categorized as information security incidents.	**ISO/IEC 27035-1:2023** **5.4 Assess and decide** **ISO/IEC 27035-3:2020** **9 Incident triage operations** **10 Incident analysis operations**

Table C.1 *(continued)*

ISO/IEC 27001:2022, Annex A	ISO/IEC 27035 series
5.26 Response to information security incidents Control: Information security incidents shall be responded to in accordance with the documented procedures.	**ISO/IEC 27035-1:2023** **5.5 Respond** **ISO/IEC 27035-3:2020** **11 Incident containment, eradication and recovery operations**
5.27 Learning from information security incidents Control: Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	**ISO/IEC 27035-1:2023** **5.6 Learn lessons** **ISO/IEC 27035-2:2023** **12 Learn lessons**
5.28 Collection of evidence Control: The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	**ISO/IEC 27035-1:2023** **5.3 Detect and report** d), i) **5.4 Assess and decide** i), l) **5.5 Respond** f), j), m)

Annex D
(informative)

Considerations of situations discovered during the investigation of an incident

In the course of incident response, there are challenging situations where the incident coordinator can play a key role in controlling and advancing the investigation process. The following items provide possible situations and actions to be taken by incident coordinator.

For the incidents, different problems can arise:

a) No underlying problem is found, and the response flows as foreseen, within the time frame. The report records all information useful for the future.

b) Discovery of one or more underlying problems. The incident coordinator decides whether or not to call up other teams who are more specialized. The resolution happens:

   — before the end of the time frame: the report records all information useful for the future;

   — potentially outside the time frame: the incident coordinator informs the targeted/affected teams/entities along with the crisis manager so that they can prepare the (re)actions.

c) Discovery of underlying problems or other potential (or affected) internal or external victims that the activated response teams can handle. The incident coordinator informs:

   — the management of a possible extension and a potential failure to conclude within the time frame; this allows for internal communication;

   — the entity entitled to communicate with the outside of the organization [press service, data protection officer (DPO), etc.] if ordered so.

d) Discovery of underlying problems or other potential (or affected) internal or external victims that the activated response teams cannot handle. The incident coordinator informs:

   — the management to activate another incident coordinator. Close coordination should then be established between the different activated capabilities and other specific response teams (e.g. physical security, external assistance, etc.);

   — the entity entitled to communicate with the outside of the organization (press service, DPO, etc.).

e) Discovery of various problems related to the SLA. The incident coordinator escalates to the crisis manager, who is responsible for:

   — informing management;

   — giving control to the crisis manager;

   — keeping informed on the incident progress (the incident coordinator takes action when needed without waiting for information);

   — activating, at request, the teams he/she controls;

   — keeping ready to take control again once the crisis is over.

Bibliography

[1] ISO 22320, *Security and resilience — Emergency management — Guidelines for incident management*

[2] ISO/IEC 20000 (all parts), *Information technology — Service management*

[3] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[4] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[5] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[6] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[7] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[8] ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[9] ISO/IEC 27031:2011, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[10] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[11] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[12] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[13] ISO/IEC 27035-2:2023, *Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

[14] ISO/IEC 27035-3, *Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations*

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

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

[17] ISO/IEC 27039, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*

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

[19] ISO/IEC 27041, *Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method*

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

[21] ISO/IEC 27043, *Information technology — Security techniques — Incident investigation principles and processes*

[22] ISO/IEC 27050 (all parts), *Information technology — Electronic discovery*

[23] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*

[24] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

[25] ISO/IEC 30121, *Information technology — Governance of digital forensic risk framework*

ICS 35.030

Price based on 33 pages