INTERNATIONAL STANDARD

ISO/IEC 27035-2

Second edition
2023-02

Information technology — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

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

Partie 2: Lignes directrices pour planifier et préparer une réponse aux incidents

Reference number
ISO/IEC 27035-2:2023(E)

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 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 27035-2:2016), which has been technically revised.

The main changes are as follows:

— the title has been modified;

— new roles including incident management team and incident coordinator and their responsibilities have been added;

— content related to vulnerability management has been modified;

— content on a recommended process for organizations has been added in 6.7;

— Clause 7 structure has been reorganized;

— C.3 has been replaced by a single paragraph;

— bibliography has been updated.

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

This document focuses on information security incident management which is identified in ISO/IEC 27000 as one of the critical success factors for the information security management system.

There can be a large gap between an organization's plan for an incident and an organization's preparedness for an incident. Therefore, this document addresses the development of procedures to increase the confidence of an organization's actual readiness to respond to an information security incident. This is achieved by addressing the policies and plans associated with incident management, as well as the process for establishing the incident response team and improving its performance over time by adopting lessons learned and by evaluation.

Information technology — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

1 Scope

This document provides guidelines to plan and prepare for incident response and to learn lessons from incident response. The guidelines are based on the "plan and prepare" and "learn lessons" phases of the information security incident management phases model presented in ISO/IEC 27035-1:2023, 5.2 and 5.6.

The major points within the "plan and prepare" phase include:

— information security incident management policy and commitment of top management;

— information security policies, including those relating to risk management, updated at both organizational level and system, service and network levels;

— information security incident management plan;

— Incident Management Team (IMT) establishment;

— establishing relationships and connections with internal and external organizations;

— technical and other support (including organizational and operational support);

— information security incident management awareness briefings and training.

The "learn lessons" phase includes:

— identifying areas for improvement;

— identifying and making necessary improvements;

— Incident Response Team (IRT) evaluation.

The guidance given in this document is generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this document 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*

ISO/IEC 27035-1:2023, *Information technology — Information security incident management — Part 1: Principles and process*

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 ISO/IEC 27035-1 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/

3.2 Abbreviated terms

CERT	computer emergency response team
CSIRT	computer security incident response team
IMT	Incident Management Team
IRT	Incident Response Team
PoC	Point of Contact

4 Information security incident management policy

4.1 General

NOTE Clause 4, in its entirety, links to ISO/IEC 27035-1:2023, 5.2 a).

An organization's information security incident management policy should provide the formally documented principles and intentions used to direct decision-making. Supporting processes and procedures ensures consistent application of the policy.

Any information security incident management policy should be part of the information security strategy for an organization. It should also support the existing mission of its parent organization and be in line with already existing policies and procedures.

An organization should implement an information security incident management policy that outlines the processes, responsible persons, authority and reporting lines when an information security event/incident occurs. The policy should be reviewed regularly to ensure it reflects the latest organizational structure, processes, and technology that can affect incident management. The policy should also outline any awareness and training initiatives within the organization that are related to incident management (see Clause 10).

An organization should document its policy for managing information security events, incidents and vulnerabilities as a free-standing document, as part of its overall information security management system policy (see ISO/IEC 27001:2022, 5.2), or as part of its information security policies (see ISO/IEC 27002:2022, 5.1). The size, structure and business nature of an organization and the extent of its information security incident management programme are deciding factors in determining which of these options to adopt. An organization should direct its information security incident management policy at every person having legitimate access to its information systems and related locations.

Before the information security incident management policy is formulated, the organization should identify the following regarding its information security incident management:

a) principles, objectives and purpose;

b) the scope, including not only which parts of the organization it applies to, but also what information it applies to e.g. hardcopy, electronic, verbal;

c) internal and external interested parties;

d) specific incident types and vulnerabilities that are controlled, responded to and resolved;

e) any specific roles that are involved;

f) benefits to the whole organization and to its departments;

g) understanding of its legal and regulatory environment;

h) dependencies including alignment to risk management;

i) skills and competency requirements.

4.2 Interested parties

A successful information security incident management policy should be created and implemented as an enterprise-wide process. To that end, all interested parties or their representatives should be involved in the development of the policy from the initial planning stages through to the implementation of any process or response team. This may include legal advisors, public relations and marketing staff, departmental managers, security staff, ICT responsible persons, upper-level management, and, in some cases, even facilities and human resources staff.

An organization should ensure that its information security incident management policy is approved by top management.

Ensuring continued management commitment is vital for the acceptance of a structured approach to information security incident management. It is important that personnel recognize an event, know what to do and understand the benefits of the approach by the organization. It is also important that management is supportive of the information security incident management policy to ensure that the organization commits to resourcing and maintaining an incident management capability.

The information security incident management policy should be made available to every employee and contractor. It should also be addressed in information security awareness briefings and training.

4.3 Information security incident management policy content

The information security incident management policy should be high-level. Detailed information and step-by-step instructions should be included in the series of documents that make up the information security incident management plan, which is outlined in Clause 6.

An organization should ensure that its information security incident management policy content addresses, but is not limited to, the following topics:

a) the purpose, objectives and the scope (to whom it applies and under what circumstances) of the policy;

b) policy owner and review cycle;

c) the importance of information security incident management to the organization, top management's commitment to it and the related plan documentation;

d) a definition of security incident;

e) a description of the type of security incidents or categories (or a reference to another document which describes this in more depth);

f) a description of how incidents should be reported, including what to report, the mechanisms used for reporting, where and to whom to report;

g) a high-level overview or visualization of the incident management process flow (showing the basic steps for handling a security incident) encompassing detection and reporting, assessment and decision, response and lessons learned;

h) a requirement for post information security incident resolution activities, including learning from and improving the process, following the resolution of information security incidents;

i) if appropriate, also a summary of reporting and handling vulnerabilities that are related to the incident (although this can be a separate document);

j) a defined set of roles, responsibilities, and decision-making authority for each phase of the information security incident management process and related activities (including reporting and handling vulnerabilities that are related to the incident if appropriate);

k) a reference to the document describing the event and incident classification, severity ratings (if used) and related terms;

l) an overview of the IMT, encompassing the IMT organizational structure, key roles, responsibilities, and authority, along with summary of duties including, but not limited to:

   1) reporting and notification requirements related to incidents that have been confirmed,

   2) dealing with enquiries, instigating follow-up, and resolving incidents,

   3) liaising with the external organizations (when necessary),

   4) requirement and rationale for ensuring all information security incident management activities performed by the IRT are properly logged for later analysis;

m) requirements for establishing/terminating IRTs to respond to specific incidents which have different scopes and expertise depending on the incident. Several IRTs may exist, depending on the aspect of business that is affected by the incident;

n) a requirement that components across the organization work in collaboration to detect, analyse, and respond to information security incidents;

o) a description of any oversight or governance structure and its authority and duties, if applicable;

p) links to organizations providing specific external support such as forensics teams, legal counsel, other IT operations, etc;

q) a summary of the legal and regulatory compliance requirements or mandates associated with information security incident management activities (for more details, see Annex A).

There are other related policies or procedures that support the information security incident management policy and can also be established as part of the preparation phase, if they are not already existent and are appropriate for the organization. These include, but are not limited to, the following:

— An information security incident management plan, described in Clause 6;

— A continuous monitoring policy for specific ICT systems stating that such activity is conducted by the organization and describing the basic monitoring tasks. Continuous monitoring ensures preservation of electronic evidence in case it is required for legal prosecution or internal disciplinary action;

— Authority granting the IRT access to the outputs of this monitoring or the ability to request logs as needed from other parts of the organization (this can also be put in the information security incident management policy);

— Information sharing, disclosure and communication policies which outline how and when information related to incident management activities can be shared by whom and with whom. Information should be kept confidential and only disclosed according to the relevant legislation. In many instances, legislation requires affected parties to be notified should any personal identifiable

information be compromised. Apart from the legal requirements, it is expected that information also follows any organizational requirements for disclosure, according to the classification policy and according to ISO/IEC 27002:2022, 5.14. It may be important to share information in the course of incident handling when a third party is involved or affected. The scope, circumstances and purpose of this information sharing are described, or referenced, in the appropriate policies and procedures. An example of information disclosure guidance and markings is the use of traffic light protocol (TLP) (see ISO/IEC 27010);

— Information storage and handling policies which require records, data, and other information related to investigations to be stored securely and handled in a manner commensurate with their sensitivity. If the organization has a document labelling or classification schema, this policy is also important to information security incident management activities and personnel;

— An IMT charter that specifies in more detail what the IMT does and the authority under which it operates;

  — At a minimum, the charter should include a mission statement, a definition of the IMT's scope, and details of the IMT's top management sponsor, the IMT authority, contact information for the IMT, its list of services and core activities, its scope of authority and operation, its purpose and goals; along with a discussion of any governance structure;

  — The goals and purposes of the team are especially important and require clear, unambiguous definition;

  — The scope of an IMT normally covers all of the organization's information systems, ICT services and networks. In some cases, an organization can require the scope to be different (either larger or narrower), in which case, it should be clearly documented what is in, and what is out of, scope;

  — Examples of IMT authority include searching and confiscating personal belongings, detaining people and monitoring communications, where possible.

— An overview of the information security incident management awareness and training programme. This should include any training mandates, policies, or requirements for staff-related employee awareness training and incident management training for the IMT members.

5 Updating of information security policies

5.1 General

NOTE Clause 5, in its entirety, links to ISO/IEC 27035-1:2023, 5.2 b).

An organization should include information security incident management content in its information security policies at the organizational level, as well as on specific ICT system, service and network levels and relate this content to the incident management policy. The integration should aim to:

a) describe why information security incident management, particularly an information security incident reporting and handling plan, is important;

b) indicate top management's commitment to the need for proper preparation and response to information security incidents, i.e. to the information security incident management plan;

c) ensure consistency across the various policies;

d) ensure planned, systematic and composed responses to information security incidents, thus minimizing the adverse consequences of incidents;

e) align with the organization’s risk management policies and practices.

For guidance on information security risk assessment and management, see ISO/IEC 27005. Policy documents should be reviewed regularly and updated when necessary. This should be a consequence of the "learn lessons" phase. See also ISO/IEC 27002:2022, 5.1.

5.2 Linking of policy documents

An organization should update and maintain its organizational information security and risk management policies, and specific system, service or network information security policies in tandem to ensure they remain consistent and current. These organizational-level policies should refer explicitly to the information security incident management policy and associated plans.

The organizational-level policies should include the requirement that appropriate review mechanisms are established. These review mechanisms should ensure that information from the detection, monitoring, resolution of and learning from information security incidents and from dealing with reported information security vulnerabilities is used as input to the process designed to maintain continuing effectiveness of the policies.

6 Creating information security incident management plan

6.1 General

NOTE 1 Clause 6, in its entirety, links to ISO/IEC 27035-1:2023, 5.2 c).

The aim of an information security incident management plan is to document the activities and procedures for dealing with information security events, incidents and related vulnerabilities discovered during an incident analysis and response, and to communicate them. The plan stems from and is based on the information security incident management policy.

Overall, the documentation of the plan should encompass multiple documents including the forms, procedures and organizational elements. It should also include support tools for the detection and reporting of, assessment and decision making related to, responses to and learning lessons from information security incidents.

The plan may include a high-level outline of the basic flow of incident management activities to provide structure and pointers to the various detailed components of the plan. These components provide the step-by-step instructions for incident handlers to follow using specific tools, following specific workflows or handling specific types of incidents based on the situation.

The information security incident management plan comes into effect whenever an information security event is detected or information security vulnerability is reported.

An organization should use the plan as a guide for:

a) detecting events and abnormal situations and reporting them;

b) responding to information security events;

c) determining whether information security events become information security incidents;

d) managing information security incidents to conclusion;

e) handling information security vulnerabilities discovered while responding to an incident;

NOTE 2 Security vulnerabilities are reported to the incident coordinator who redirects them to the team responsible for vulnerability management.

f) requirements for reporting;

g) requirements for recording information (including its format) during the whole incident management process;

h) rules and circumstances under which information sharing with internal and external groups or organizations can take place;

i) identifying lessons that can be learned, and any improvements to the plan and/or security in general that are required.

Planning and preparation of an incident management plan should be undertaken by the process owner, with a clear goal or set of goals for incident response within a defined scope based on the information security incident management policy.

6.2 Information security incident management plan built on consensus

This document recommends the development of an information security incident management policy. However, where there is no guiding policy or standard, prevailing law, or other authoritative source, the incident management planning process should be based on consensus to ensure effective operation, communication, and relationships with external organizations.

Terms and definitions should be normalized between the organization and partner organizations where relevant. This includes names and identifiers for organizations and teams, information assets and business processes. Where terminology is difficult or prone to misinterpretation, the incident management plan should include standard terms and definitions in a glossary.

Roles and relationships with external IRTs and other response organizations, as well as response activity structures and boundaries should be defined by the incident management process owner. Responsibilities of interested parties can overlap and should be adjusted by consensus in the incident management planning process. Where there is overlap on incident response decision boundaries, the plan should identify a responsible party.

Interested parties and external IRTs often have disparate metrics. Planning participants should evaluate the available metrics contributed by their respective parties or external organizations and either agree by consensus on particular set(s) of existing metrics or agree to link the disparate metrics using a reversible mapping. Regardless of approach, the plan should select or connect quantitative metrics so that their scopes are identical and select or connect qualitative metrics with definitive equivalence.

6.3 Interested parties

An organization should ensure that the information security incident management plan is acknowledged by all personnel and associated contractors, ICT service providers, telecommunication providers and outsourcing companies, thus covering the following responsibilities:

a) detecting and reporting information security events (this is the responsibility of any permanent or contracted personnel in an organization and its companies);

b) assessing and responding to information security events and incidents, being involved in the post-incident resolution activities of learning, and improving information security and the information security incident management plan itself (this is the responsibility of interested parties including the PoC (point of contact), the incident coordinator, the IRT, management, public relations personnel and legal representatives);

c) dealing with information security vulnerabilities (this is the responsibility of skilled members from vulnerability management).

The plan should also take into account any third-party users. Consideration should be given to information security incidents and associated vulnerabilities reported from third party organizations, government and commercial information security incident and vulnerability information provision organizations.

If interested parties are expected to be actively involved in handling information security incidents, then a clear division of roles and responsibilities should be made and everyone made aware of them.

Division of roles should be accompanied with the agreed incident handoff protocol so that information is exchanged in an expedient manner. If appropriate and possible, the incident handoff and information exchange should be automated to speed up the process. This kind of scenario can arise if some of the organization or IRT capabilities are outsourced to a third party. Examples include when the organization uses cloud systems run by the third party, or when the third party performs digital forensics for the organization, or when the organization works with a service provider in handling incidents.

6.4 Information security incident management plan content

Key decision-making criteria and processes to support expected management phases should be defined and reviewed before the planning and preparation process. This requires available policy, formal or informal understanding of assets and controls, and contribution from participants and management support.

The content of the information security incident management plan should give an overview, as well as specifying detailed activities. As noted above, the plan documentation should encompass multiple documents including the forms, procedures, organizational elements and support tools.

The detailed activities, procedures and information should consider the following.

a) Plan and prepare.

   1) A standardized approach to information security event/incident categorization and classification, to enable the provision of consistent results. In any event, the decision should be based on the actual or projected adverse consequences on the organization's business operations, harm to individuals/other organizations and associated guidance;

      NOTE Annex C shows example approaches to the categorization and classification of information security events and incidents.

   2) An information security incident register structured for the exchange of information is likely to provide the capability to share reports/alerts, compare results, improve alert information and enable a more accurate view of the threats to, and vulnerabilities of information systems. The actual format and use of the incident register depend on the organization’s requirements. For example, a very small organization may use documents, while a complex organization may use more sophisticated technology such as relational databases and application tools;

   3) Guidance for deciding whether escalation is required during each relevant process, and to whom, and associated procedures. Based on the guidance provided in the information security incident management plan, the incident coordinator should know under which circumstances it is necessary to escalate matters and to whom it should be escalated. In addition, there are unforeseen circumstances when this may be necessary. For example, a minor information security incident can evolve to a significant or a crisis situation if not handled properly or a minor information security incident not followed up timely can become a major information security incident;

   4) Procedures to be followed to ensure that all information security incident response activities are properly logged and that log analysis is conducted by designated personnel;

   5) Procedures and mechanisms to ensure that the change control regime is maintained covering information security event, incident and related vulnerability tracking and information security report updates, and updates to the plan itself;

   6) Procedures for information security evidence recording, safeguarding and analysis;

   7) Procedures for handover to law enforcement when a crime occurs;

   8) On ICT systems, procedures and guidance on using intrusion detection systems (IDS) and intrusion prevention systems (IPS), ensuring that associated legal and regulatory aspects have been addressed. Guidance should include discussion of the advantages and disadvantages

of undertaking attacker surveillance activities. Further information on IDS is contained in ISO/IEC 27039;

9) Guidance and procedures associated with the technical and organizational controls and mechanisms that are established, implemented and operated in order to prevent information security incident occurrences and to reduce their likelihood, and to deal with information security incidents as they occur;

10) Material for the information security event, incident and vulnerability management awareness and training programme;

11) Procedures and specifications for the testing of the information security incident management plan;

12) Organizational structure for information security incident management;

13) The terms of reference and responsibilities of the IMT, IRT and incident coordinator;

14) Important contact information;

16) Procedures and guidance regarding information sharing as agreed with the organization's public affairs office, legal department and top management or relevant departments;

17) Establishing and maintaining the list of information security events and incidents the organization wants to be able to detect, respond to and learn from as the result of the information security risk treatment phase.

b) Detect and report.

1) Planning and preparation requirements for detection and reporting should enable and support the development and operation of processes to find or accept information about information security incidents;

2) Criteria for acceptance of an event report should be defined, based on the completeness of the report and verification of one or more information security events. To support later decision-making, minimum criteria for acceptance of any event detection alert or manual report should be defined prior to the planning process. It should include at least identification of an affected environment or asset, a statement of one or more suspected or confirmed events or qualified event type, and the time received. In order to support decision making, the planning process should include a method for returning detection or reports that have insufficient information;

3) Reporting output or notification should be defined in the context of the organization, the incident response procedures, and assignment of technical and management roles. The format of reports and notification should match the incident classification scale or a consistent related metric;

4) The event report should be generic, but contain as much information as possible based on a clear template everyone understands and can complete;

5) Detecting and reporting the occurrence of information security events (by human or automatic means);

6) Collecting the information on information security events;

7) Detecting and reporting on information security vulnerabilities;

8) Recording information gathered in the information security incident register.

c) Assess and decide.

1) Planning and preparation requirements for assessment and decision should enable and support the development and operation of processes to evaluate and direct actions in response to information security incidents;

2) Prior to development of assess and decide processes, the process owner should ensure that the minimum information for identification and classification of a security incident is defined, consisting of specific items of required and supporting information. This definition allows response planners to develop consistent processes for completeness and classification of detected and reported events. The information required to differentiate between true positive and false positive reports should be defined and allow for accumulation of information to support estimation of and response to false negative detection and reports within specific ICT systems;

3) If the incident planning process is to depend on automated information management and decision support systems, the functions, implementation, and on-going operation of these systems should be defined. An information security incident register should be sufficiently defined prior to developing the response processes that depend on it;

4) Conducting assessments of information security events (including escalation as required), using the information security event/incident classification scale (including determining the impacts of events based on the affected assets/services) should decide whether events should be classified as information security incidents. To do this, assessments should be conducted using the information security event/incident classification scale to confirm the details of the event (suspected incident) type and affected resource (categorization). This should be followed by making decisions on how the confirmed information security incident should be dealt with, by whom and in what priority, as well as escalation levels;

5) Fully recording all assessment results and related decisions in the information security incident register;

d) Respond.

1) Planning and preparation requirements for response should enable and support the development and operation of processes to respond to information security incidents. Prior to response planning, the incident manager should gather information on the security incident, including priority of information and information system, impact of each intrusion types, damage scale, intrusion alarm level, and severity. These can be qualitative or quantitative, as long as they are consistent with assess and decide preparations, and enable the incident coordinator to assign the incident actions or tasks to responders;

2) The classification of response should also be defined prior to the planning process, organized by cost, time, technical resource minimums, and other metrics to enable assignment of response class relative to the known information about the assessed incident. Immediate or deferred response should be included, as well as a definition of how single or cyclic incident tasks is managed in the response process;

3) Defining a map of all internal and external functions and organizations that should be involved during the response of an incident;

4) Determining and documenting what should be done to contain and eradicate the information security incident as appropriate to mitigate or prevent the scope and impact of the incident from increasing;

5) Determining and documenting how to identify, collect/acquire, analyse and preserve electronic evidence;

6) Determining the conditions, the procedure to escalate along with all interested parties involved;

7) Determining the process and format to ensure that all associated activities are properly logged for later analysis;

8) Determining the process to forward the necessary information to the organizational and ICT change management capability;

9) Determining the channel and format to communicate the existence of the information security incident or any relevant details thereof to other internal and external people or organizations;

10) Assessing information security vulnerabilities that are discovered during incident response and dealing with these information security vulnerabilities with the help of vulnerability management capability;

11) Determining and documenting the process to close the incident with approval of the process owner(s) impacted by the incident, to record this in the information security incident register and to notify results to all interested parties;

12) Determining the conditions requiring further analysis and documenting what should be done;

13) An organization should ensure that the information security incident management plan documentation allows for information security incident responses, both immediately and longer-term. All information security incidents should undergo an early assessment of the potential adverse consequences on business operations, both short and longer-term (for example, a significant disruption can occur sometime after an initial information security incident). Furthermore, it should allow for some responses necessary for information security incidents that are completely unforeseen, where immediate interim controls are required. Even for this situation, organizations should encompass general guidelines in the plan documentation on the steps that can be necessary.

e) Learn lessons.

1) Determining and documenting how to learn lessons from information security incidents and how to propose improvements to incident management;

2) Ensuring that the change control regime (organizational and IT change management) is triggered and maintained;

3) Updating the information security incident register;

4) Communicating and sharing the results of review within a trusted community (if the organization so wishes).

6.5 Incident classification scale

An information security event/incident classification scale should be used to grade events/incidents. In any event, the decision should be based on the actual or projected adverse consequences on the organization's business operations, individuals or other organizations.

NOTE Annex C shows examples of approaches to the categorization, evaluation and prioritization of information security events and incidents.

6.6 Incident forms

Incident forms should be created before they are needed. The number, type and format of the forms should be determined by the IMT or relevant authority and revised periodically to ensure their continued relevance. An open space for descriptive text should exist. Its purpose is to provide a mechanism to capture information in instances where existing forms are not sufficient or an appropriate form has not yet been created. It is recommended to have a list of facts/situations that can be considered as an event/incident.

Forms should be advertised and made available for the users so that a person reporting an information security event is familiar with them.

Example forms are shown in Annex B.

In large and interconnected ICT systems, it is recommended that internationally standardized formats for the electronic exchange and input of incident information are used, linking directly to the electronic

information security database. Using standardized electronic exchange format allows increased automation in processing data and can reduce effort in correlating information when multiple teams cooperate on handling an incident. A paper-based scheme may be needed for a case where an electronic scheme cannot be used.

6.7 Documented processes and procedures

Before commencing operation of the information security incident management plan, it is important that an organization has documented and checked that necessary processes and procedures are available. Each document should indicate those groups or individuals responsible for its use and management.

A list of possible incidents that the organization wishes to be able to manage should be established and maintained. This list is mainly based on the result of risk assessments. For each incident, the organization should:

— determine activities to be carried out to adequately respond and foresee a supposed duration (that is verified during a test and re-evaluated at each execution of the response process);

— determine the facts/devices that enable detection of the event occurrence;

— determine the data to be gathered in the event report;

— determine the skills of the response teams;

— determine which workarounds allow the restart of business activities;

— determine the resources needed for the response team to intervene;

— determine the resolution conditions to be validated by the impacted business owner;

— test/evaluate the procedure;

— determine, install and operate the automated detection devices.

It is important to understand that not all documents should be readily available either within the organization or to the general public. For example, it is not necessary for all organizational personnel to understand the internal operation of an IMT in order to interact with it. The IMT should ensure that available guidance, including information resulting from information security incident analysis, is in readily available form, e.g. on the organization's intranet and/or public website, as appropriate. It may also be important to keep some details of the information security incident management plan closely held to prevent an insider from tampering with the investigation process. For example, if bank employees who are embezzling funds are aware of some details on how the investigation is being done, they can better hide their activities from investigators, or hamper the detection, investigation of and recovery from an information security incident.

The content of operating procedures depends on a number of criteria, especially related to the nature of known potential information security events, incidents and vulnerabilities and the types of information system assets that are involved and their environment. Thus, an operating procedure can be related to a particular type of incident or product (for example, firewalls, databases, operating systems, applications) or to a specific ICT product. Each operating procedure should clearly identify the steps to be undertaken and by whom. It should reflect experience from external (for example, government and commercial IRTs or similar, and suppliers), as well as from internal sources. These operating procedures should also cover non-ICT issues such as confidentiality, privacy breach, theft, physical intrusion, power supply defect that can harm ICT systems.

There should be operating procedures for dealing with types of information security events and incidents that are already known, as well as involved vulnerabilities. There should also be operating procedures to follow when an identified information security event, incident or involved vulnerability is not of any known type. In this case, the following should be addressed:

a) the reporting process for the handling of such exceptions;

b) guidance on the timing for getting approval from management in order to avoid any delay of response;

c) delegation by default for decision making.

Operating procedures for the IRT should be developed with documented processes and associated responsibilities and the allocation of roles to designated persons to conduct various activities, including, for example:

— shutting down an affected system, service and/or network, in certain circumstances agreed by prior arrangement with the relevant IT and/or business management;

— leaving an affected system, service and/or network, connected and running;

— monitoring data flowing from, to and within an affected system, service and/or network;

— activating normal back-up procedures and actions in line with the system, service and/or network security policy;

— monitoring and maintaining the secure preservation of electronic evidence, in case it is required for legal prosecution or internal disciplinary action;

— communicating information security incident details to internal and external people or organizations. This may include communicating with several types of outside parties such as other incident response teams, information sharing organizations, internet service providers, software and support vendors, law enforcement agencies, customers, media, regulators and other relevant parties. All contacts and communications with outside parties should be documented for liability and evidentiary purposes;

— isolating access to hardcopy records;

— monitoring physical access to facilities.

6.8 Trust and confidence

The IMT plays a crucial role for the overall information security of an organization. The IMT requires the collaboration of all organizational personnel to detect, resolve and investigate information security incidents. It is fundamental that the IMT is trusted by the whole organization and that external entities have confidence in it. The trust within the organization is created through authority and stems from the support given by the top management. External entities that deal with the incidents should be confident that the IMT performs its job professionally.

The IMT can earn trust through transparency and mature processes. The IMT should work to educate users (internal and external), explain how the IMT works, how it protects the confidentiality of information collected and how it manages security event, incident and vulnerability reports. The IMT should document and publicize provisions that clearly illustrate the expectation of anonymity, or lack thereof, for persons or parties reporting a suspected information security incident or vulnerability.

The IMT should be capable of efficiently satisfying the functional, financial, legal and political needs of the organization and be able to exercise organizational discretion when managing information security incidents and vulnerabilities. The function of the IMT should also be independently audited to confirm that all business requirements are being satisfied effectively.

Furthermore, a good way of achieving another aspect of independence is to separate the incident and vulnerability reporting chain from operational line management and to make a top manager directly responsible for managing incident and vulnerability responses. Finance of the capability should also be segregated to avoid undue influence.

6.9 Handling confidential or sensitive information

An information security incident management plan may contain sensitive information and people involved in addressing incidents and vulnerabilities may be required to handle sensitive information. An organization should ensure that the necessary processes and capabilities are established to protect sensitive information when required (e.g. when leaving the protective domain of the IMT, in application of the control in ISO/IEC 27002:2022, 5.10). If information security events/incidents/vulnerabilities are logged via a generalized problem management system where it is not possible to restrict who has access to it, sensitive details may have to be obfuscated. Given that the IMT would still require access to the omitted information, this can lead to a situation where the IMT maintains its own information security incident register.

As outlined elsewhere in this document, an organization should also ensure that the information security incident management plan makes provision for controlling the communication of incidents and vulnerabilities to external parties, including the media, business partners, customers, law enforcement organizations, regulators and the general public.

7 Establishing an incident management capability

7.1 General

NOTE Clause 7, in its entirety, links to ISO/IEC 27035-1:2023, 4.5.3).

The aim of establishing an incident management organizational structure is to provide the organization with appropriate capability for assessing, responding to and learning from information security incidents, and providing the necessary coordination, management, feedback and communication. This incident management organizational structure contributes to the reduction in physical and monetary damage, as well as the reduction of other business impacts such as harm to individuals, legal and regulatory impact, service delivery impact, the damage to the organization's reputation that is sometimes associated with information security incidents.

Incident management organizational structure can be structured differently depending on the organization size, its staff members and industry type.

7.2 Incident management team establishment

7.2.1 IMT structure

An incident management team (IMT) is the group responsible for managing the end to end incident management capability for the organization. As leader of an IMT, the incident manager should be close to the top management and refer to them regularly, as the top management makes the final decision to approve plans and engage the necessary resources. The incident manager is primarily responsible for building and managing the incident management policy and plan. The incident manager should have the necessary soft skills to lead an IMT of various competencies and should also have capacities for project management, especially when information security incident management is new to the organization.

The main activities of IMT may include, but are not limited to, the following.

— Managing integrated security systems: monitoring information security event management agents installed on heterogeneous systems (e.g. intrusion detection system, intrusion prevention system, firewall, network resource, etc.).

— Implementing a consistent policy: minimizing risks to the information system by applying a consistent set of response tasks according to the defined policy.

— Responding promptly: defining the most appropriate detection and response mechanisms to react quickly to threats, breaches, and attacks to minimize damage and reduce cost of recovery.

Duties of an IMT may also include monitoring and management activities as follows.

— Integrated management and monitoring: 24 h × 365 d monitoring of targets, proactive monitoring and responses against incidents, log management.

— Reports management: periodic security reporting, security patch management, incident reporting.

— Administrative management: policy management for various system environments including task control and IRT operations.

— Technical management: network, system, application, contents, and service security management.

— System operation and management: system capacity, performance, security configuration, and environment configuration management.

NOTE Some of the above duties can be shared with or performed by other organizational units outside of the IMT.

7.2.2 IMT roles and responsibilities

To organize an IMT, the roles of members can be defined as shown in Table 1. Some of these tasks can be shared with or performed by other organizational units outside of the IMT. The IMT may provide input but do not have ultimate authority.

Table 1 — Example roles and tasks of IMT staff members

Role	Description
Incident manager	The leadership role is responsible for managing the staff members, defining the job scope, and reporting the status to top management.
Planning team	It establishes or plans various security policies, reports them to higher-level authorities, cooperates with third parties, and registers and approves vulnerability reports. Its responsibilities are as follows: a) planning and establishing security policies; b) implementing security processes; c) adjusting the risk priorities; d) communicating with other organizations; e) supporting administration; f) discussing/registering/approving vulnerability reports on the target organizations; g) preparing and organizing awareness and training programmes; h) performing other activities directed by the incident manager.
Monitoring team	When an automated system is in place to monitor and detect anomalies, responsible for real-time monitoring and actual operation activities such as security event monitoring/detection/identification, incident registration, and prevention. It performs the real-time security monitoring activities and the following: a) 24 h × 365 d monitoring and operation; b) intrusion detection, registering incidents, and first responses; c) undertaking triage of events/incidents; d) performing the security patches and upgrades; e) implementation of the security policy and backup management; f) help desk; g) facility management; h) performing other activities directed by the incident manager.
Analysis team	In cooperation with the response team, it performs in-depth analysis including correlation analysis for the incidents. Analysis on incidents and the following are also provided: a) planning vulnerability analysis for the target organization and IRT; b) improving the security analysis tools and checklist; c) improving the monitoring rules; d) publication of newsletter; e) performing other activities directed by the incident manager.
Test and evaluation team	Responsible for organizing and performing incident response process and procedures tests.

Table 2 provides an example of the types of staffing, the range of positions and the tasks for various positions that may be required for an IMT.

Table 2 — Example IMT staff positions

Staff title	Tasks
Manager or team leader	— provides strategic direction — enables and facilitates work of team members — supervises team — represents IMT to management and others — interviews and hires new team members
Assistant managers, supervisors, or group leaders	— support strategic direction of assigned functional area — support the team leader as needed — provide direction and mentoring to team members — assign tasks and duties — participate in interviews to recruit new team members
Help desk or triage staff	— handle main PoC telephone(s), email mailboxes, reporting portal etc. for incident or security reports — provide initial assistance, depending on skills — undertake initial data entry and the sorting and prioritizing of incoming information
Technical writers	— assist and facilitate the IMT in the development of publications such as advisories, best practices, or technical tips

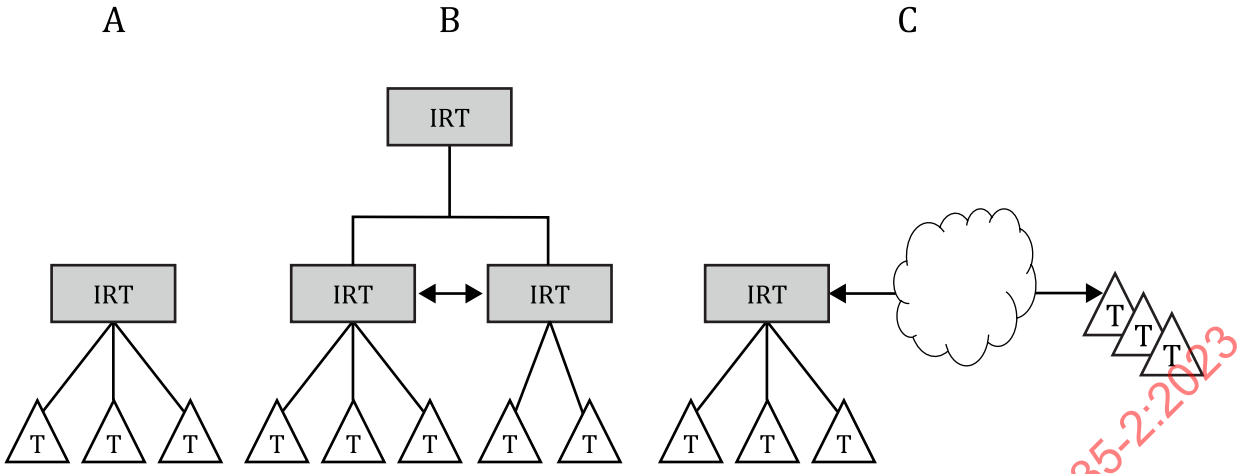
7.3 Incident response team establishment

7.3.1 IRT structure

Incident response teams (IRT) are set up and disbanded as incidents arise. The members and size of the IRT vary depending on the incident they are responding to. For example, an incident related to stolen hard copy documents may include facilities management and HR representatives, while a ransomware incident requires the expertise of the IT department and possibly external providers.

The IRT(s) is led by an incident coordinator who oversees the activities throughout the respond phase including regular reporting to the incident manager of the IMT and interested parties. The incident coordinator also recommends when the IRT has completed its activities and the team can be disbanded.

IRTs can be structured various ways, including by sector, constituency focus, organizational structure, or by other attributes. One method of structure is via the type of monitoring scope, in which case, there are three different types as shown in Figure 1; single, hierarchical, and remote. To establish an IRT, the size of the organization, the importance of the information and interoperability with other organizations should be considered. In Figure 1, the T refers to targets which are monitored by the particular IRT.



Key

A single

B hierarchical

C remote

T targets monitored by the IRT

Figure 1 — Example IRT structures

— Single (single type of IRT): the monitoring scope is a single organization, or a single IRT performing monitoring of multiple organizations or targets. This type is generally used for the incident management, response and operation activities.

— Hierarchical (hierarchical type of IRT): one or more IRTs overlap monitoring scopes. It can increase the reliability for incident response activities.

— Remote (remote type of IRT): By collecting the security events from remote locations, this type is generally used for out-sourcing enterprises (specialized information security enterprises) to monitor the targets.

7.3.2 IRT types and roles

An incident response team (IRT) should have a defined constituency for which it is primarily responsible. The characteristics and size of the constituency and the level of authority and control the incident response team has over its members affects the types of service the IRT can offer and the appropriate form of organization to deliver it. For example, IRTs may themselves do hands-on incident response (either in-house or as a contracted service), they may coordinate the work of other IRTs, or they may provide information and assist individual members on request (e.g. product IRTs).

Whatever services it offers, the IRT requires a response policy (defining what constitutes an incident, what response(s) is/are required and what authority the IRT is responsible for delivering it), a response process (defining how the team responds to those incidents to deliver that response), and operational capabilities to implement that process.

The incident coordinator has the crucial role of leading the response until the incident is officially closed after confirmation by the impacted services. The responsibilities of incident coordinator are as follows:

— evaluate the event and decide, based on the procedure and the determined evaluation criteria, if it becomes an incident;

— coordinate the work of the IRTs and communicate with them to keep continuously informed of the situation;

— communicate with the incident manager and impacted business managers to inform them on the evolution of the situation;

— communicate with external interested parties as defined in the incident response procedures;

— log all decisions and actions made during the incident response;

— verify with the owner/manager of the impacted business entity if the “incident closure” conditions are fulfilled;

— build, complete and communicate the incident response.

The responsibilities of the IRT include:

— manage the case from the monitoring agents for incidents related to intrusion, theft, data exfiltration or exposure, perform secondary further analysis and actions including investigation efforts, perform recovery actions and establish adequate strategy;

— communicate with the incident coordinator on any vulnerabilities or unusual situations discovered during the response activities;

— communicate with the incident coordinator on the evolution of their activities;

— perform the collection and safeguarding of the tracks and evidences as directed by the incident coordinator;

— perform the post-incident activities as directed by the incident coordinator;

— undertake incident analysis, tracking, recording, and response;

— undertake technology-watch activities, if assigned;

— develop appropriate training materials (for IRT staff and/or the constituency);

— mentor new IRT staff, as assigned;

— monitor intrusion detection systems, if this service is part of the IRT activities;

— perform penetration testing if this service is part of the IRT activities;

— participate in interviews to recruit new staff members as directed.

7.3.3 IRT staff competencies

Effective incident response depends on the capability and reliability of IRT staff members. Skills required for IRT members may include the following.

a) Personal skills: communication, problem solving, team interactions, time and project management;

b) Technical skills: security principles, risks analysis, threat modelling, vulnerability analysis, log analysis;

c) Incident response skills: team policy/procedure, communication, incident analysis, recording and tracking incident information;

d) Specialized skills: presentation, leadership, subject matter expertise.

In order to respond to various types of incidents which relates to ICT, where relevant, IRT members should possess technical knowledge and skills such as:

— current network security issues, including attacks, threats, malware, and vulnerabilities;

— system administration security practices such as patch management, secure configuration, backup, and disaster recovery;

— cryptography (encryption and hash algorithms), digital signatures, current protocols such as Secure Sockets Layer protocol/ Transport Layer Security protocol (SSL/TLS);

— common network protocols such as ethernet (IEEE 802.3), Wireless Fidelity (WiFi, IEEE 802.11), Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP);

— common network application protocols such as Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), HTTP(S);

— digital evidence collection, reverse engineering;

— computer science and programming concepts such as entropy, secure development, functional and object-oriented programming, system architecture and memory layout.

Other specific knowledge and skills should be determined by duties of the IRT and technology used by the organization. The examples in this list are current at the time this document was developed. IRT members should maintain current knowledge and skills.

8 Establishing internal and external relationships

8.1 General

NOTE Clause 8, in its entirety, links to ISO/IEC 27035-1:2023, 5.2 e).

It is important to establish and preserve appropriate relationships and connections with internal and external organizations that are directly involved in information security event, incident and vulnerability management.

8.2 Relationship with other parts of the organization

Incident management is not a self-contained process. Relationships, communication channels, data sharing agreements, and policies and procedures should be established across the organization. These internal collaborations can include the following.

— Business managers: They should understand what the IMT and IRT are and how they can help support their business processes. Agreements should be made concerning the authority of the IMT and IRT over business systems and who makes decisions if critical business systems are disconnected from the network or shut down;

— Representatives from IT: The interactions and workflow between the IT staff and the IMT/IRTs should be defined. These include what actions are taken by IT staff, what actions are taken by IMT and IRTs members, what information the IT staff can provide to the IMT and IRTs, what information the IMT and IRTs can provide to the IT team, and what roles, responsibilities and authority each have;

— Representatives from the legal department: These representatives can provide guidance on liability and compliance issues, identify if service level agreements (SLAs) are not impacted during an incident and provide guidance on privacy and civil liberties to ensure investigation and response actions do not infringe on employee rights. They should also provide advice on which incidents constitute mandatory data breach notifications, when to inform the regulator(s), who informs the regulator(s) on the organization's behalf and how they inform the regulator(s);

— Representatives from human resources: It is important that they are involved in developing policies and procedures for managing internal employees found engaging in unauthorized or illegal computer activity;

— Representatives from public relations: They should be prepared to handle any media inquiries and help develop information disclosure policies and practices;

— Any existing security groups, including physical security and data protection: It is important that the IMT and incident coordinator exchange information with these groups about information security incidents, and may share responsibility with them for resolving issues involving computer or information theft;

— Audit and risk management specialists: They can help develop threat metrics and identify risks to constituency systems;

— Any law enforcement liaisons or investigators: They understand how the team should work with law enforcement, when to contact law enforcement and who does the investigations and forensic analysis;

— General representatives from the constituency: They can provide insight into their needs and requirements;

— Crisis management/business continuity: These workflows should be established between these two groups along with rules for escalation of incidents to crisis management and a feedback mechanism at the closure of an incident to enable up to date records for the incident management team.

The incident coordinator and IRTs should be responsible for ensuring that incidents are resolved. In this context, the incident coordinator and IRT members should have a degree of authority to take the necessary actions deemed appropriate in response to information security incidents. However, actions that can have adverse effects on the overall organization, either financially or in terms of reputation, should be agreed to by top management. For this reason, it is essential that the information security incident management policy and plan detail the appropriate management function to which the incident coordinator reports serious information security incidents. The management function, on its part, should make a commitment to be available to the incident coordinator and deliver its guidance in a timely fashion.

Procedures and responsibilities for dealing with the media should also be agreed to by top management and documented. These procedures should specify who in the organization deals with media inquiries, and how that part of the organization interacts with the IMT.

8.3 Relationship with external interested parties

Organizations should establish relationships between the IMT and appropriate external interested parties. IMT and incident coordinator should regularly communicate with outside parties regarding an incident, whenever appropriate, such as contacting law enforcement, fielding media inquiries, and seeking external expertise. Another example is discussing incidents with other interested parties, such as internet service providers (ISPs), the vendor of vulnerable software or other incident response teams. With the approval of incident coordinator or incident manager, IRTs may also proactively share relevant incident indicator information with peers to improve detection and analysis of incidents.

Information should only be communicated with external parties in accordance with organizational and incident management policies and processes.

NOTE Legal or regulatory requirements can apply.

IRT members should seek to join trusted communities of colleagues in the IRT field of practice to increase their professional acumen and create trusting relationships for information exchange. Exchanging technical information with trusted partner IRTs in the detect and report phase of incident handling can improve response effectiveness and help to minimize impacts on other organizations. As many cybersecurity threats affect multiple organizations simultaneously, this type of information sharing is considered crucial for responsible IRT operations. Where practical, automated exchanges of incident information should be established to increase the speed at which new incidents can be detected through collective IRT activity.

External interested parties can include (but are not limited to) the following:

a) contracted external support personnel;

b) IMTs and IRTs of external organizations;

c) managed service providers (including telecommunication service providers), ISPs, vendors and suppliers;

d) law enforcement organizations;

e) emergency authorities;

f) CERTs[1)] and CSIRTs, where appropriate;

g) appropriate government organizations, or data protection agency;

h) legal personnel;

i) public relations officials and/or members of the media;

j) business partners;

k) customers;

l) general public;

m) regulators.

9 Defining technical and other support

9.1 General

NOTE 1 Clause 9, in its entirety, links to ISO/IEC 27035-1:2023, 5.2 f).

To ensure that quick and effective responses to information security incidents can be achieved, an organization should acquire, prepare and test all necessary technical and other support means. All internal and external parties for support and reporting should be defined and communication channels and workflow agreed upon. These activities include the following:

— access to details of the organization's assets with an up-to-date asset register and information linkage to business functions including the asset owner;

— documented and promulgated communications processes including media communications procedures that comply with the organization's policies on media interaction and information disclosure. For example, an organization may want members of its public affairs office and legal department to participate in all incident discussions with the media;

— the use of an information security incident register and the means to populate and update the register quickly, analyse its information and facilitate responses (in some instances manual records can be required by an organization), with the register kept demonstrably secure;

— the use of a standard format and exchange protocol to receive and process alerts or information on events/incidents/vulnerabilities to inform situational awareness of the information security operating environment, allowing for risk-based and proactive remediation;

— resources/tools for information security/digital evidence collection and analysis;

— adequate crisis management documentation and arrangements (for guidance on business continuity management, see ISO/IEC 27031, ISO 22301 and ISO 22313);

— defining external parties for support and reporting, and defining point of contacts between the organizations including how and when to communicate.

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.

An organization should ensure that the technical means support the following:

a) quick acquisition of information security event/incident/vulnerability reports;

b) notification of previously selected external personnel by appropriate means, thus requiring a contact register (including paper and other backups) with all required details (e.g. person, position, e-mail, telephone, group e-mail), and the appropriate means to transmit information to individuals in a secure fashion where appropriate;

c) taking precautions commensurate with assessed risks for ensuring that electronic communication, whether internet or non-internet, cannot be eavesdropped and stays available while the system, service and/or network is under attack (this can require pre-planned alternative communications mechanisms being in place);

d) ensuring the collection of all information about the incident including any supporting information system, service and/or network, and all information both stored and processed appropriately;

e) using cryptographic integrity control to help in determining whether and what parts of the system, service and/or network, and what data, were changed, if commensurate with assessed risks;

f) facilitating the archiving and securing of collected information (for example, by applying digital signatures to logs and other evidence before storing in appropriate off-line storage, also see ISO/IEC 27040);

g) enabling the preparation of printouts (e.g. of logs), including those showing the progress of an incident, and the resolution process and chain of custody;

h) recovery of the information, information system, service and/or network to normal operation, with the following procedures that are in line with the relevant crisis management:

   1) backup testing;

   2) malicious code control;

   3) original media with system and application software;

   4) bootable media;

   5) clean, reliable and up-to-date system and application patches;

   6) transfer of recovered physical files/tamper proof containers, safe hand delivery protocols;

   7) copies of hardcopy records.

Organizations can create a standard baseline image from the installation media and use it as the clean basis for creating systems. Using such an image instead of the original media is often preferable because the image has already been patched, hardened, tested, etc.

An attacked information system, service or network may not function correctly. Thus, as far as possible, no technical means (software and hardware) necessary for responding to an information security incident should rely in their operations on the organization's “mainstream” systems, services and/or networks, proportionate to the assessed risks. All technical means should be carefully selected, correctly implemented and regularly tested (including testing of the backups made). If it is possible, the technical means should be fully independent.

NOTE 2 Technical means described in this subclause do not include technical means used to detect information security incidents and intrusions directly and to automatically notify appropriate persons. Such technical means are described in ISO/IEC 27039.

9.2 Technical support

Technical support mechanisms can include the following:

a) internal information security audit mechanisms to assess the security level and track vulnerable systems;

b) vulnerability management (including security updates and security patching of vulnerable systems);

c) technology tracking to detect new kinds of threats and attacks;

d) intrusion detection systems (for more details, see ISO/IEC 27039);

e) network security devices, protections means and monitoring tools (for more details, see the ISO/IEC 27033 series);

f) anti-malware software;

g) audit log records, and log monitoring software.

9.3 Other support

Other support mechanisms can include documented responsibilities and operating procedures for the operations support team. Examples of other technical support may include use of electronic evidence collection and forensic tools (whether sourced internally or outsourced).

10 Creating information security incident awareness and training

NOTE Clause 10, in its entirety, links to ISO/IEC 27035-1: 2023, 5.2 g).

Information security incident management is a process that involves not only technical means but also people. Therefore, it should be supported by appropriately information security-aware and trained individuals within the organization (also noted in ISO/IEC 27002:2022, 6.3).

The awareness and participation of all organization personnel is crucial for the success of a structured information security incident management approach. Users should be made aware of how they and their department can benefit from participating in a structured approach to information security incident management. Furthermore, the operational efficiency and quality of a structured approach to information security incident management relies on a number of factors, including obligation to notify interested parties of incidents, quality of notification, ease of use, speed and training. Some of these factors relate to making sure that users are aware of the value of information security incident management and being motivated to report incidents.

The organization should ensure that the role of information security incident management is actively promoted as part of the organizational information security awareness and training programme. The awareness programme and related material should be available to all personnel, including new employees, third party users and contractors, as relevant. There should be a specific training programme or programmes for the PoC, IRT members, information security personnel and specific administrators, as necessary. Each group of people involved directly with the management of incidents can require different levels of training, depending on the type, frequency and criticality of their interaction with the information security incident management plan.

The organization's awareness briefings should encompass the following:

a) benefits to be derived from the structured approach to information security incident management, both to the organization and to its personnel;

b) how the information security incident management plan works, including its scope and the security event, incident and vulnerability management workflow;

c) how to report on information security events, incidents and vulnerabilities;

d) incident information held in, and the outputs from, the information security incident register;

e) controls on confidentiality of sources as relevant;

f) notification of outcomes, under what circumstances sources are advised;

g) any constraints imposed by non-disclosure agreements;

h) the authority of the information security incident management organization and its reporting line;

i) who receives reports from the information security incident management plan and how the reports are distributed.

The response teams should know what to do, which resources to use and in which time frames. It is essential that the personnel be trained to perform with efficiency and calm.

Training should at least be focused on:

— event evaluation procedure;

— event detection and raising;

— incident response;

— swift bidirectional passage to and from crisis management.

The organization should make personnel aware of, and train them to detect information events. The organization should make them understand that raising information events is firstly not a source of penalties (even if the "finder" is the cause of the event), and secondly is handled anonymously.

In some cases, it may be desirable for the organization to include awareness detail specifically about information security incident management in other training programmes (for example, personnel orientation programmes or general organizational security awareness programmes). This awareness approach can provide valuable context relevant to particular groups of people and improves training programme effectiveness and efficiency.

Before the information security incident management plan becomes operational, the organization should ensure that all relevant personnel are familiar with the procedures involved in the detection and reporting of information security events, and selected personnel are very knowledgeable about the subsequent activities. This should be followed up by regular awareness briefings and training courses. The training should be supported by specific exercises and testing for PoC and IRT members and information security personnel and specific administrators.

In addition, the awareness and training programmes should be complemented by the establishment and operations of "hot line" support from information security incident management personnel, in order to minimize delays in reporting and handling information security events, incidents and vulnerabilities.

11 Testing the information security incident management plan

11.1 General

NOTE Clause 11, in its entirety, links to ISO/IEC 27035-1:2023, 5.2 h).

The organization should schedule regular checking and testing of the information security incident management processes and procedures to highlight potential flaws and problems that can arise during the management of information security events, incidents and related vulnerabilities. Periodic tests should be organized to check processes/procedures and to verify the incident response responses. These simulated scenarios can range from severe, complex incidents based on realistic attacks, failures or faults to table top exercises. The format of the simulation depends on the pre-defined goals of the

exercise. Tests can involve not only the IRT, but also some or all internal and external organizations that are involved in the management of information security incidents. Organizations should ensure that any changes made as a result of post testing reviews are subject to thorough checking, including further testing, before the changed plan goes live.

When conducting an exercise, it is very important that all involved are aware that they are not dealing with the real attack. It is important to establish and maintain this difference to prevent people from triggering actions that may have much larger implications to the organization (e.g. initiate building evacuation). This rule can be ignored only under special circumstances when the exercise is performed within strictly controlled environment that prevents the effects of the exercise to "spill over" into the operational environment.

Every exercise goes through the following phases:

— planning and preparation;

— execution;

— debrief and post incident analysis.

Planning and preparation of an exercise is based on the current incident management plans and envisaged future threats and trends. The results of the post-incident analysis are used as input to improve the incident management plans.

11.2 Exercise

11.2.1 Defining the goal of the exercise

Generally speaking, an exercise can have the following three main goals:

a) validation: to validate incident management plans and identify potential omissions or errors;

b) training: to allow people to practice their roles and make them comfortable executing them;

c) testing: to test the currently existing processes and procedures.

It is common that an exercise has more than one goal. The goal of an exercise is in good part determined by the overall state of preparedness of the organization. When an organization is preparing new incident management plans or updating the existing ones, it can use exercises to validate them. After the plans are made and put in place, the organization uses exercises to train the people. After the existing processes and procedures are well established, they should be periodically tested to ensure that they are still valid.

Table 3 is given as guidance on what types of exercises can be used to achieve which goal(s).

Table 3 — Mapping exercise goals to exercise types

Goal	Exercise types
Validating new plans	discussion-based table top
Training people	discussion-based table top live (e.g. real acting out simulation using actual systems red/blue teaming/social engineering activities)
Verifying if the existing plans are still valid	table top live

11.2.2 Defining the scope of an exercise

The scope of an exercise is mainly defined by its goals. When defining the scope of an exercise, the following items should be considered:

a) whether the exercise involves only internal people (within the organization) or external organizations;

b) exactly who is involved, i.e. is it the IRT only, or are people from other groups included, and if so, which groups;

c) how many exercise leaders are required.

The scope has direct influence on which organizations are represented at the exercise and profile of the participants.

11.2.3 Conducting an exercise

When conducting an exercise, it is very important that all involved are aware that the scenario being handled is an exercise and not a real event. If participants are unable to distinguish simulated from the real events, there is potential that they trigger actions with wider consequences or involve people outside of the exercise. In the worst case scenario, this can lead to panic in the general public.

There are number of tasks that should be accomplished in order to conduct a successful exercise. The following list provides only a general overview of the main tasks:

a) at the beginning, brief participants on the exercise goals;

b) ensure safety and security of all participants (this is especially important with live exercises where volunteers are used);

c) make sure that all participants know their roles;

d) ensure that appropriate people, e.g. incident manager along with the incident coordinator and business representative depending on the incident being tested, are available to lead participants through the exercise;

e) allocate sufficient time for discussion during the exercise but not an excessive amount to derail the exercise;

f) allow sufficient time and resources to debrief all participants after the exercise and collect their feedback (note that the feedback is twofold: what was the objective of the exercise and how the exercise itself was conducted);

g) create and distribute exercise reports to the interested parties.

11.3 Incident response capability monitoring

11.3.1 Implementing an incident response capability monitoring programme

Incident response capabilities encompass not only capabilities of the incident response team, but also capabilities of the individuals and groups that IRT may ask for help during the incident handling. While most of the incident response capabilities are concentrated within the IRT, it is possible that it can lack specialist knowledge in certain narrow areas. For that reason, the IRT may engage individuals or other teams to fill this void.

By monitoring characteristics of incidents and frequency by which these characteristics occur in incidents, it is possible to develop a picture of what capabilities the IRT should possess. These capabilities change over time. Some changes occur because technology within the organization is either abandoned or new technology is introduced. An example of abandoning technology may be moving all data from SQL databases to non-SQL databases. Allowing employees to use mobile telephones to

perform their tasks is an example of introducing a new technology that previously did not exist within the organization. Another reason that can lead to change in IRT capabilities is the development of new attack techniques.

Not all capabilities are technical in nature. Some threats, especially ones that do not rely on technology, are best addressed with non-technical means (e.g. social engineering).

11.3.2 Metrics and governance of incident response capability monitoring

The IRT capabilities should be adequate to address the current threats facing the organization. As the threats change, so does the team capabilities so that the organization can effectively respond to the new threats. At the same time, some capabilities may no longer be needed as the threats are either permanently reduced to negligible levels or the underlying reason for the risk has been removed. Additionally, while the IRT should be the focal centre of the expertise and the main bearer of incident handling capabilities, it is not essential to possess all of them. Rarely used expertise and capabilities can be distributed among different individuals or groups either within or outside of the organization. The main reason for this is cost-effectiveness.

With such distribution of capabilities and changing needs, the organization should establish a register that would reflect its current capabilities. The following non-exhaustive list illustrates information that can be contained in this register:

a) capabilities available to the organization;

b) who possesses such capabilities;

c) whether the bearers of the capabilities are internal or external to the organization;

d) how to engage the bearer of the capability;

e) types of threats this capability can be used to respond/reduce/eliminate;

f) how current is the capability (or its proxy measure when it was last used);

g) how often the capability was required in the past time interval.

This information is then used in the planning of development of IRT capabilities. Rarely used capabilities can be left to lapse and often used capabilities not currently present within the IRT can be gained.

12 Learn lessons

12.1 General

NOTE Clause 12, in its entirety, links to ISO/IEC 27035-1:2023, 5.6.

Once an information security incident has been handled and closed, the organization should identify and learn lessons, and ensure that the conclusions are acted upon. Furthermore, lessons can be learned from the assessment and resolution of reported information security vulnerabilities or after testing the information security incident management plan. Where necessary, the following statistics are updated:

— Mean time between incidents. If the tendency decreases after a few incidents, a study should be necessary to discover where and why the organization is more exposed or vulnerable;

— Mean time between same type of incidents (e.g. technical attack, malware, compromise of information). If the tendency decreases after a few incidents, a study should be necessary to discover the reason;

— Mean time to resolve same type of incidents. If the tendency increases after a few incidents, a study is necessary to discover the reason.

Decisions on lessons learned should be based on the risk induced with the result of the incident report analysis.

12.2 Identifying areas for improvement

An organization should look beyond a single information security incident or vulnerability and check for trends/patterns for which they can help identify the need for controls or changes. It is also sensible practice following an IT-oriented information security incident, to conduct information security testing, particularly vulnerability assessment. Thus, an organization should analyse the data in the information security incident register on a regular basis in order to do the following:

— identify trends/patterns;

— identify areas of concern;

— analyse where preventive action can be taken to reduce the likelihood of future incidents.

Relevant information acquired throughout the course of an information security incident should be channelled into the trend/pattern analysis (similar to the way reported information security vulnerabilities are handled). It contributes significantly to the early identification of information security incidents and provides a warning of further information security incidents which can arise, based on previous experience and documented knowledge.

Information security incident and related vulnerability information received from government, other IRTs and suppliers should also be used.

Summary analyses of information security incidents and vulnerabilities should be produced for tabling at each meeting of the organization's management information security forum and/or other forum defined in the overall organizational information security policy. For more information on vulnerability handling, see ISO/IEC 30111.

12.3 Identifying and making improvements to the information security incident management plan

As a part of post-incident resolution, the incident coordinator should review all that has happened to assess and thus quantify the effectiveness of the entire response to an information security incident. Such an analysis aims to determine which parts of the information security incident management plan worked successfully and identify if any improvements are required.

An important aspect of post response analysis is to feed information and knowledge back into the information security incident management plan. If an incident is sufficiently severe, an organization should ensure that a meeting of all the relevant parties is scheduled shortly after its resolution while information is still fresh in people's minds. Factors to consider in such a meeting include the following.

a) Did the procedures outlined in the information security incident management plan work as intended?

b) Are there any procedures or methods that would have aided in the detection of the incident?

c) Were any procedures or tools identified that would have been of assistance in the response process?

d) Were there any procedures that would have aided in recovering information and systems following an incident identified?

e) Was the communication of the incident to all relevant parties effective throughout the detection, reporting and response process?

The results of the meeting should be documented. The organization should ensure that the areas identified for improvement to the information security incident management plan are reviewed and justified changes incorporated into an update of the plan documentation. The changes to the

information security incident management processes, procedures and the reporting forms should be subject to thorough checking and testing before going live.

12.4 IMT evaluation

Compared to learn lessons, an evaluation is a periodic and more holistic assessment of the effectiveness of the IMT. Once the IMT has been in operation, the team and its management should evaluate the effectiveness of the team and how well it meets the needs of the constituency. An evaluation can be conducted periodically or aspects of evaluation can be integrated into operational and learn lessons processes.

Examples of evaluation activities include the following:

— determining which activities work well and which do not;

— evaluating the capabilities and services once they become operational;

— checking how the IMT is doing with the constituency and any external partners and collaborators.

Examples of more specific feedback mechanisms include the following:

a) benchmarking;

b) general discussions or interviews with representatives from the constituency and external partners and collaborators;

c) surveys distributed on a periodic basis to constituency members;

d) creation of a set of criteria or quality parameters that is then used by an audit or third-party group to evaluate the IMT.

Performance metrics can also be collected to help evaluate IMT success. Possible metrics can include, but are not limited to, the following:

— incident statistics, such as counts of different types of incidents, response times, incident life times, resolution or disposition of incidents;

— amount of information reported to constituency about information security issues or ongoing activity;

— preventative techniques and security practices in place.

Any changes and improvements should be based on outcomes of the evaluation.

12.5 Identifying and making improvements to information security control implementation

During review, after one or more information security incidents and related vulnerabilities have been resolved, new or changed controls may be identified as being required. The recommendations and related control requirements can be such that it is not financially or operationally feasible to implement them immediately, in which case, they should feature in the longer-term aims of the organization. For example, migration to a more secure and robust firewall may not be financially feasible in the short term, but should be factored into an organization's long-term information security goals.

In accordance with the agreed recommendations, the organization should implement the updated and/or new controls. These can be technical (including physical) controls and can include the need for rapid material updates for, and delivery of, security awareness briefings (for users, as well as other personnel), and rapid revision and issue of security guidelines and/or standards.

In addition, while reviews of information security-related procedures and documentation can be conducted in the immediate aftermath of an information security incident, it is more likely that this is

required as a later response. Following an information security incident, if relevant, an organization should update its information security policies and procedures to take into account information gleaned and any problems identified during the course of the incident management process. It should be a long-term aim of the IMT, in conjunction with the organization's information security manager, to ensure that these information security policy and procedural updates are propagated throughout the organization.

Other improvements may have been identified during the learn lessons phase, for example, changes in information security policies, standards and procedures, personnel security controls and changes to IT hardware and software configurations. Personnel security controls may include implementing more rigorous employment screening processes when engaging personnel or implementing regular ongoing personnel checks. The organization should ensure that these are acted upon.

A special case of lessons learned is the analysis of a non-standard application of the information security incident management plan. This situation can arise if the reporting processes are used for reporting events like IT problems (e.g. computer or application malfunction), misconduct within the organization (whistleblowers) or other events not related to information security. Increased instances of such use can signify problems in other parts of the organization or insufficient training on the proper purpose and use of the reporting processes. A potential result of this analysis can be to highlight deficiencies in other, non-security related processes or parts of the organization, to top management.

12.6 Identifying and making improvements to information security risk assessment and management review results

Depending on the severity and impact of an information security incident (or the severity and potential impact to a reported related information security vulnerability), an assessment of information security risk assessment and management review results can be necessary to consider new threats and vulnerabilities. This includes reviewing the consequence levels in the risk assessment with the actual consequence levels that occurred during the incident/as a result of the incident to make sure they align with the previously assessed likelihood and consequence levels. As a follow-up to the completion of an updated information security risk assessment and management review, it may be necessary to introduce changed or new controls (see 11.3 and ISO/IEC 27005).

12.7 Other improvements

Sometimes analysing an incident can produce results that are not strictly related to incident management, but can help with streamlining operation of an organization or other improvements. The following list is given as an illustration of such improvements and is by no means exhaustive or exclusive:

— delay in providing fixes/patches can lead to refining criteria for selecting software or hardware vendors;

— insufficient staffing availability during handling of the incident due to inadequate resource planning can be corrected by provision of adequate staff levels, enhanced education and training and timely deployment of required system enhancements.

Annex A
(informative)

Considerations related to legal or regulatory requirements

A.1 Introduction

Legal or regulatory requirements often apply in the context of information security incident management. Consequently, the following aspects should be addressed in the information security incident management policy and associated scheme.

A.2 Data protection and privacy of personal information

Adequate data protection and privacy of personal information is provided. In those countries where specific legislation exists that covers data confidentiality and integrity, it is often restricted to the control of personal data. As information security incidents are typically attributed to an individual, it is important that information of a personal nature is therefore recorded and managed accordingly. A structured approach to information security incident management therefore takes into account the appropriate privacy protection. This may include the following:

a) those individuals with access to the personal data should, so far as is practical, not personally know the person(s) being investigated;

b) non-disclosure agreements should be signed by those individuals with access to the personal data prior to them being allowed access to it;

c) information should only be used for the specific purpose for which it has been obtained, i.e. for information security incident investigation.

A.3 Record keeping

Appropriate record keeping is maintained. Some national laws require that companies maintain appropriate records of their activities for review in the annual organization audit process. Similar requirements exist with regard to government organizations. In certain countries, organizations are required to report or to generate archives for law enforcement (e.g. regarding any case that may involve a serious crime or penetration of a sensitive government system).

A.4 Controls to ensure fulfilment of commercial contractual obligations

It is presupposed that controls are in place to ensure fulfilment of commercial contractual obligations. Where there are binding requirements on the provision of an information security incident management service, for example covering required response times, it is presupposed that appropriate information security is provided to ensure that such obligations can be met in all circumstances. Related to this, if an organization contracts with an external party for support, for example an external IRT, then it is presupposed that all requirements, including response times, are included in the contract with the external party.

A.5 Legal issues related to policies and procedures

Legal issues related to policies and procedures are dealt with. It is presupposed that the policies and procedures associated with the information security incident management scheme are checked for

potential legal or regulatory issues, for example if there are statements about disciplinary and/or legal action taken against those causing information security incidents.

A.6 Disclaimers are checked for legal validity

Disclaimers are checked for legal validity. It is presupposed that all disclaimers regarding actions taken by the information incident management team and any external support personnel, are checked for legal validity.

A.7 Contracts with external support personnel

Contracts with external support personnel cover all required aspects. It is presupposed that contracts with any external support personnel, for example from an external IRT, are thoroughly checked regarding waivers on liability, non-disclosure, service availability, and the implications of incorrect advice.

A.8 Non-disclosure agreements

Non-disclosure agreements are enforceable. Information security incident management team members may be required to sign non-disclosure agreements both when starting and leaving employment. In some countries, having signed non-disclosure agreements may not be effective in law; it is presupposed that this is checked.

A.9 Law enforcement requirements

Law enforcement requirements are addressed. It is presupposed that the issues associated with the possibility that law enforcement agencies legally request information from an information security incident management scheme are clear. It may be necessary to clarify the minimum legal requirements for documenting incidents and how long that documentation should be retained.

A.10 Liability aspects

Liability aspects are clear. It is presupposed that the issues of potential liability and related required controls are clarified. Examples of events which may have associated liability issues are as follows:

a) if an incident can affect another organization (for example, disclosure of shared information, and it is not notified in time and the other organization suffers an adverse impact);

b) if a new vulnerability in a product is discovered and the vendor is not notified and a major related incident occurs later with major impact other organizations;

c) a report is not made where, in the particular country, organizations are required to report to or generate archives for law enforcement agencies regarding any case that may involve a serious crime, or penetration of a sensitive government system or part of the critical national infrastructure;

d) information is disclosed that seems to indicate that someone, or an organization, may be involved in an attack. This can damage the reputation and business of the person or organization involved;

e) information is disclosed that there may be a problem with a particular item of software and this is found not to be true.

A.11 Specific regulatory requirements

Specific regulatory requirements are addressed. Where required by specific regulatory requirements, it is presupposed that incidents are reported to a designated body, for example as required in the nuclear power industry, telecommunications companies and internet service providers in many countries.

A.12 Prosecutions, or internal disciplinary procedures

Prosecutions, or internal disciplinary procedures, can be successful. It is presupposed that appropriate information security controls are in place, including provably tamper-proof audit trails, to be able to successfully prosecute, or bring internal disciplinary procedures against, “attackers”, whether the attacks are technical or physical. In support of this, it is presupposed that evidence is collected in a manner that is admissible in the appropriate national courts of law or other disciplinary forum. It should be possible to show that:

a) records are complete and have not been tampered with in any way;

b) copies of electronic evidence are provably identical to the originals;

c) any IT system from which evidence has been gathered was operating correctly at the time the evidence was recorded.

A.13 Legal aspects

Legal aspects associated with monitoring techniques are addressed. It is presupposed that the implications of using monitoring techniques are addressed in the context of the relevant national legislation. The legality of different techniques vary from country to country. For example, in some countries, people are made aware that activities are monitored, including through surveillance techniques. Factors that can be considered include who/what is being monitored, how they/it are being monitored, and when the monitoring is occurring. Monitoring/surveillance in the context of IDS is specifically discussed in ISO/IEC 27039.

A.14 Acceptable use policy

Acceptable use policy is defined and communicated. It is presupposed that acceptable practice/use within the organization is defined, documented and communicated to all intended users. For example, it is presupposed that users are informed of the acceptable use policy and asked to provide written acknowledgement that they understand and accept that policy when they join an organization or are granted access to information systems.

Annex B
(informative)

Example forms for information security events, incidents and vulnerability reports

B.1 Introduction

This annex contains examples of items which are recorded for information security events, incidents and vulnerabilities. It also contains examples of forms for reporting on information security events, incidents and vulnerabilities, with related notes. It is emphasized that these are examples. There are other examples, such as the schema from incident object description and exchange format (IODEF) standard.

B.2 Example items in records

B.2.1 Example items of the record for information security event

This includes basic information on the information security event, such as when, what, how and why the event occurred, as well as the contact information of the reporting person.

- Basic information
  - Date of event
  - Event number
  - Related event and/or incident numbers (if applicable)
- Reporting person details
  - Name
  - Contact information such as address, organization, department, telephone and e-mail
- Event description
  - What occurred
  - How it occurred
  - Why it occurred
  - Initial views on components/assets affected
  - Adverse business impacts
  - Any vulnerability identified
- Event details
  - Date and time the event occurred
  - Date and time the event was discovered
  - Date and time the event was reported

B.2.2 Example items of the record for information security incident

This includes basic information on the information security incident, such as when, what, how and why the incident occurred, as well as the incident category, impact, and result of incident response.

- Basic information
  - Date of incident
  - Incident number
  - Related event and/or incident numbers (if applicable)
- Reporting person
  - Name
  - Contact information such as address, organization, department, telephone and e-mail
- Point of Contact (PoC) member
  - Name
  - Contact information such as address, organization, department, telephone and e-mail
- IRT member details
  - Name
  - Contact information such as address, organization, department, telephone and e-mail
- Incident description
  - What occurred
  - How it occurred
  - Why it occurred
  - Initial views on components/assets affected
  - Adverse business impacts
  - Any vulnerability identified
- Incident details
  - Date and time the incident occurred
  - Date and time the incident was discovered
  - Date and time the incident was reported
- Incident category
- Components/assets affected
- Adverse business impact/effect of incident
- Total recovery cost from incident
- Incident resolution
- Person(s)/perpetrator(s) involved (if incident caused by people)
- Description of perpetrator

— Actual or perceived motivation

— Actions taken to resolve incident

— Actions planned to resolve incident

— Actions outstanding

— Conclusion

— Internal individuals/entities notified

— External individuals/entities notified

B.2.3 Example items of the record for information security vulnerability

This includes basic information on the information security vulnerability, such as when, what and how the vulnerability was identified, as well as the potential impact and the resolution.

— Basic information

  — Date of vulnerability identified

  — Vulnerability number

— Reporting person details

  — Name

  — Contact information such as address, organization, department, telephone and e-mail

— Vulnerability description

— Vulnerability resolution

B.3 How to use forms

B.3.1 Format of date and time

Dates should be entered in the format YYYY-MM-DD (and if required HH-MM-SS). If relevant, coordinated universal time (UTC) should be used for ready comparison when many events are occurring across time zones (and at the least state the UTC offset applied to the time). See the ISO 8601 series for further information.

B.3.2 Notes for completion

The purpose of the information security event and incident report form is to provide information about an information security event. If it is determined to be an information security incident, information about the incident should be provided to the appropriate people.

If an information security event is suspected to be in progress or have occurred — particularly one which may cause substantial loss or damage to the organization's property or reputation — an information security event report form should be immediately completed and submitted in accordance with the procedures described in the information security incident management plan of the organization.

The information provided is used to initiate appropriate assessment, which determines whether the event is classified as an information security incident or not, and if it is any remedial measures necessary to prevent or limit any loss or damage. Given the potentially time-critical nature of this process, it is not essential to complete all fields in the reporting form at this time.

If a PoC member reviews the already completed/partially completed form, then a decision is made as to whether the event is classified as an information security incident. If an event is classified as such, the

information security incident form should be completed with as much information as possible. Both the information security event and incident forms should be forwarded to the IRT. Whether the information security event is classified as an incident or not, the incident management system should be updated.

If an IRT member reviews information security event and incident forms forwarded by a PoC member, then the incident form should be then updated as the investigation progresses, and related updates made to the incident management system.

The purpose of the information security vulnerability report form is to provide information about a perceived vulnerability, and to act as the repository of information on the resolution of the reported vulnerability.

Please observe the following guidelines when completing the forms:

— It is recommended that the form is completed and submitted electronically.

NOTE This includes a secure web page form with linkage to the electronic information security event/incident/vulnerability database. Although operating a paper-based plan would be time consuming, a paper-based plan is also critical, in preparation for situations where it is not possible to use an electronic plan.

— When problems exist, or are considered to exist, with electronic reporting mechanisms (e.g. e-mail), including when it is thought possible that the system is under attack and report electronic forms can be read by unauthorized people, then alternative means of reporting should be used. Alternative means can include in person, by telephone or text messaging.

— Only factual information should be provided. There should be no speculation in order to complete fields. Where it is necessary to provide unconfirmed information, it should be clearly stated that the information is unconfirmed, and why this may be the case.

— Full contact details should be provided. It may be necessary to contact the person who submitted the report or form — either urgently or at a later date — to obtain further information.

If it is later discovered that any information provided is inaccurate, incomplete or misleading, the form should be amended and re-submitted.

B.4 Example forms

B.4.1 Example form for information security event report

Information Security Event Report

1. Date of event	**Page 1 of 1**
2. Event number [a]	**3. (If applicable) Related event and/or Incident Identity Numbers**

[a] Event numbers should be allocated by the organization's IRT Manager.

4. REPORTING PERSON DETAILS

4.1 Name		**4.2 Address**	
4.3 Organization		**4.4 Department**	
4.5 Telephone		**4.6 E-mail**	

5. INFORMATION SECURITY EVENT DESCRIPTION

5.1 Description of the event:

— What occurred

— How it occurred

— Why it occurred

— Initial views on components/assets affected

— Adverse business impacts

— Any vulnerabilities identified

6. INFORMATION SECURITY EVENT DETAILS

6.1 Date and time the event occurred

6.2 Date and time the event was discovered

6.3 Date and time the event was reported

6.4 Is the response to this event closed? **YES** ☐ **NO** ☐

(tick as appropriate)

6.5 If yes, specify how long the event has lasted in days/hours/minutes

B.4.2 Example form for information security incident report

Information Security Incident Report

1. Date of incident

Page 1 of 6

2. Incident number [a]

[a] Incident numbers should be allocated by the organization's IRT Manager, and linked to the associated event numbers.

3. (If applicable) Related event and/or incident identity numbers

4. POINT OF CONTACT MEMBER DETAILS

4.1 Name	**4.2 Address** .....
4.3 Organization	**4.4 Department** .....
4.5 Telephone	**4.6 E-mail** .....

5. IRT MEMBER DETAILS

5.1 Name	**5.2 Address** .....
5.3 Organization	**5.4 Department** .....
5.5 Telephone	**5.6 E-mail** .....

6. INFORMATION SECURITY INCIDENT DESCRIPTION

6.1 Further description of the incident:

— What occurred

— How it occurred

— Why it occurred

— Initial views on components/assets affected

— Adverse business impacts

— Any vulnerabilities identified

7. INFORMATION SECURITY INCIDENT DETAILS

7.1 Date and time the incident occurred

7.2 Date and time the incident was discovered

7.3 Date and time the incident was reported

7.4 Identity/contact details of reporting person

7.5 Is the incident over? *(tick as appropriate)* **YES** ☐ **NO** ☐

7.6 If yes, specify how long the incident has lasted in days/hours/minutes

Information Security Incident Report

Page 2 of 6

8. INFORMATION SECURITY INCIDENT CATEGORY

(Tick one, then complete related section below.) **8.1 Actual** ☐ *(incident has occurred)*

8.2 Suspected ☐ *(incident thought to have occurred but not confirmed)*

(One of) **8.3 Natural disaster** ☐ *(indicate threat types involved)*

☐ **Earthquake** ☐ **Volcano** ☐ **Flood** ☐ **Violent wind**

☐ **Lightning** ☐ **Tsunami** ☐ **Collapse** ☐ **Other**

Specify:

***(One of)* 8.4 Social unrest** ☐ *(indicate threat types involved)*

☐ **Terrorist assault** ☐ **War** ☐ **Other**

Specify:

***(One of)* 8.5 Physical damage** ☐ *(indicate threat types involved)*

☐ **Fire** ☐ **Water** ☐ **Electrostatic**

☐ **Abominable environment (such as pollution, dust, corrosion, freezing)**

☐ **Destruction of equipment** ☐ **Destruction of media** ☐ **Theft of equipment**

☐ **Theft of media** ☐ **Loss of equipment** ☐ **Loss of media**

☐ **Tampering with equipment** ☐ **Tampering with media** ☐ **Other**

Specify:

(One of) **8.6 Infrastructure failure** ☐ *(indicate threat types involved)*

☐ **Power-supply failure** ☐ **Networking failure** ☐ **Air-conditioning failure**

☐ **Water-supply failure** ☐ **Other**

Specify:

(One of) **8.7 Radiation disturbance** ☐ *(indicate threat types involved)*

☐ **Electromagnetic radiation** ☐ **Electromagnetic pulse** ☐ **Electronic jamming**

☐ **Voltage fluctuation** ☐ **Thermal radiation** ☐ **Other**

Specify:

(One of) **8.8 Technical failure** ☐ *(indicate threat types involved)*

☐ **Hardware failure** ☐ **Software malfunction**

☐ **Overloading (saturating the capacity of information systems)**

☐ **Breach of maintainability** ☐ **Other**

Specify:

Information Security Incident Report

8. INFORMATION SECURITY INCIDENT CATEGORY

(One of) **8.9 Malware** ☐ *(indicate threat types involved)*

☐ **Computer virus** ☐ **Network worm** ☐ **Trojan horse** ☐ **Botnet**

☐ **Blended attacks** ☐ **Malicious code embedded web page**

☐ **Malicious code hosting site** ☐ **Ransomware** ☐ **Other**

Specify:

(One of) **8.10 Technical attack** ☐ *(indicate threat types involved)*

☐ **Network scanning** ☐ **Exploitation of vulnerability** ☐**Exploitation of backdoor**

☐ **Login attempts** ☐ **Interference** ☐ **Denial of Service (DoS)**

☐ **Domain hijacking** ☐ **Other**

Specify:

(One of) **8.11 Breach of rule** ☐ *(indicate threat types involved)*

☐ **Unauthorized use of resources** ☐ **Breach of copyright** ☐ **Other**

Specify:

(One of) **8.12 Compromise of functions** ☐ *(indicate threat types involved)*

☐ **Abuse of rights** ☐ **Forging of rights** ☐ **Denial of actions** ☐ **Mis-operations**

☐ **Breach of personnel availability** ☐ **Other**

Specify:

*(One of)***8.13 Compromise of information** ☐ *(indicate threat types involved)*

☐ **Interception** ☐ **Spying** ☐ **Eavesdropping** ☐ **Disclosure**

☐ **Masquerade** ☐ **Social engineering** ☐ **Network phishing** ☐ **Theft of data**

☐ **Loss of data** ☐ **Tampering with data** ☐ **Data error** ☐ **Data flow analysis**

☐ **Position detection** ☐ **Other**

Specify:

(One of) **8.14 Harmful contents** ☐ *(indicate threat types involved)*

☐ **Illegal contents** ☐ **Terroristic contents** ☐ **Malicious contents**

☐ **Abusive contents** ☐ **Other**

Specify:

8.15 Others ☐ *(If not yet established whether incident belongs to the above category, tick here)*

Specify:

9. COMPONENTS/ASSETS AFFECTED [a]

[a] This is for more details of the components/assets affected, if available, as the investigation and analysis proceeds (in the early stages of event and incident analysis, normally only "high level" information is collected).

Components/ Assets affected *(if any)*	*(Provide descriptions of the components/assets affected by or related to the incident, including serial, license and version numbers where relevant.)*