INTERNATIONAL STANDARD

ISO/IEC 27035-2

First edition
2016-11-01

Information technology — Security techniques — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

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

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

Reference number
ISO/IEC 27035-2:2016(E)

© ISO/IEC 2016

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **2**
3.1 Terms and definitions 2
3.2 Abbreviated terms 2

4 Information security incident management policy **3**
4.1 General 3
4.2 Involved parties 3
4.3 Information security incident management policy content 4

5 Updating of information security policies **6**
5.1 General 6
5.2 Linking of policy documents 6

6 Creating information security incident management plan **6**
6.1 General 6
6.2 Information security incident management plan built on consensus 7
6.3 Involved parties 8
6.4 Information security incident management plan content 8
6.5 Incident classification scale 12
6.6 Incident forms 12
6.7 Processes and procedures 12
6.8 Trust and confidence 13
6.9 Handling confidential or sensitive information 14

7 Establishing an incident response team (IRT) **14**
7.1 General 14
7.2 IRT types and roles 14
7.3 IRT staff 16

8 Establishing relationships with other organizations **19**
8.1 General 19
8.2 Relationship with other parts of the organization 19
8.3 Relationship with external interested parties 20

9 Defining technical and other support **20**
9.1 General 20
9.2 Examples of technical support 22
9.3 Examples of other support 22

10 Creating information security incident awareness and training **22**

11 Testing the information security incident management plan **24**
11.1 General 24
11.2 Exercise 24
11.2.1 Defining the goal of the exercise 24
11.2.2 Defining the scope of an exercise 25
11.2.3 Conducting an exercise 25
11.3 Incident response capability monitoring 26
11.3.1 Implementing an incident response capability monitoring program 26
11.3.2 Metrics and governance of incident response capability monitoring 26

12 Lessons learned **27**
12.1 General 27
12.2 Identifying the lessons learned 27

© ISO/IEC 2016 – All rights reserved

12.3 Identifying and making improvements to information security control implementation 28
12.4 Identifying and making improvements to information security risk assessment and management review results 28
12.5 Identifying and making improvements to the information security incident management plan 28
12.6 IRT evaluation 29
12.7 Other improvements 30

Annex A (informative) **Legal and regulatory aspects** **31**

Annex B (informative) **Example information security event, incident and vulnerability reports and forms** **34**

Annex C (informative) **Example approaches to the categorization and classification of information security events and incidents** **46**

Bibliography **57**

 © ISO/IEC 2016 – All rights reserved

4 Information security incident management policy

4.1 General

NOTE Clause 4, in its entirety, links to ISO/IEC 27035-1:2016, 5.2 a).

An organization information security incident management policy should provide the formally documented principles and intentions used to direct decision-making and ensure consistent and appropriate implementation of processes, procedures, etc. with regard to this 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 (specifically the primary point of contact for reporting suspected incidents) when an information security incident occurs. The policy should be reviewed regularly to ensure it reflects the latest organizational structure, processes, and technology that can affect incident response. The policy should also outline any awareness and training initiatives within the organization that is related to incident response (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 27001:2013, 5.2), or as part of its Information Security Policies (see ISO/IEC 27002:2013, 5.1.1). The size, structure and business nature of an organization and the extent of its information security incident management program 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) objectives;

b) interested parties internally and externally;

c) specific incident types and vulnerabilities that need to be highlighted;

d) any specific roles that need to be highlighted;

e) benefits to the whole organization and to its departments.

4.2 Involved parties

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

An organization should ensure that its information security incident management policy is approved by a member of top management, with commitment from all of top management.

Ensuring continued management commitment is vital for the acceptance of a structured approach to information security incident management. Personnel need to recognize an incident, know what to do and understand the benefits of the approach by the organization. Management needs to be supportive of the information security incident policy to ensure that the organization commits to resourcing and maintaining an incident response capability.

© ISO/IEC 2016 – All rights reserved

The information security incident management policy should be made available to every employee and contractor and 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 and top management's commitment to it and the related plan documentation.

d) A definition of what a security incident is.

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) from detection, through reporting, information collection, analysis, response, notification, escalation, and resolution.

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 vulnerability reporting and handling (although this could be a separate policy document).

j) Defined set of roles, responsibilities, and decision-making authority for each phase of the information security incident management process and related activities (including vulnerability reporting and handling if appropriate).

k) A reference to the document describing the event and incident classification, severity ratings (if used) and related terms. The overview should either contain a description of what constitutes an incident or a reference to the document where that is described.

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

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

    2) briefing top management on incidents;

    3) dealing with enquiries, instigating follow up, and resolving incidents;

    4) liaising with the external organizations (when necessary);

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

m) A requirement that components across the organization work in collaboration to detect, analyse, and respond to information security incidents.

 © ISO/IEC 2016 – All rights reserved

n) A description of any oversight or governance structure and its authority and duties, if applicable.

o) Links to organizations providing specific external support such as forensics teams, legal counsel, other IT operations, etc.

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

q) A list and reference to other policies, procedures, and documents that support the information security incident management process and related activities. Many of the items listed in the policy may have their own more detailed procedures or guidance documents.

There are other related policies or procedures that will support the information security incident management policy and could also be established as part of the preparation phase, if they don't already exist and if they 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 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 operation (this could 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 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, information should also follow any organizational requirements for disclosure. Information may need to be shared in the course of incident handling when a third party needs to be involved or modified. The scope, circumstances and purpose of this information sharing need to be 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). An example of TLP guidance can be seen at https://www.us-cert.gov/tlp.

— 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 will also be important to information security incident management activities and personnel.

— An IRT charter that specifies in more detail what the IRT is to do and the authority under which it operates. At a minimum, the charter should include a mission statement, a definition of the IRT's scope, and details of the IRT's top management sponsor, the IRT authority, contact information for the IRT, 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 IRT normally covers all of the organization's information systems, 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 IRT authority include searching and confiscating personal belongings, detaining people and monitoring communications.

  — IRT governance might include the identification of an executive officer, board member or top manager who has the authority to make decisions on IRT and also establish the levels of authority

© ISO/IEC 2016 – All rights reserved

for IRT. Knowing this helps all personnel in the organization to understand the background and set-up of the IRT and it is vital information for building trust in the IRT. It should be noted that before this detail is promulgated, it should be checked from a legal perspective. In some circumstances, disclosure of a team's authority can expose it to claims of liability.

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

5 Updating of information security policies

5.1 General

NOTE Clause 5, in its entirety, links to ISO/IEC 27035-1:2016, 5.2 b).

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

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

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

c) To ensure consistency across the various policies.

d) To ensure planned, systematic and calm responses to information security incidents, thus minimizing the adverse impacts of incidents.

For guidance on information security risk assessment and management, see ISO/IEC 27005.

5.2 Linking of policy documents

An organization should update and maintain its corporate 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 corporate-level policies should refer explicitly to the information security incident management policy and associated plans.

The corporate-level policies should include the requirement that appropriate review mechanisms need to be established. These review mechanisms need to ensure that information from the detection, monitoring and resolution of 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 Clause 6, in its entirety, links to ISO/IEC 27035-1:2016, 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 vulnerabilities, and communication of them. The plan stems from and is based on the information security incident management policy.

 © ISO/IEC 2016 – All rights reserved

Overall, the plan documentation should encompass multiple documents including the forms, procedures, organizational elements and 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 will 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 the following:

a) responding to information security events;

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

c) managing information security incidents to conclusion;

d) responding to information security vulnerabilities;

e) requirements for reporting;

f) requirements for storing information (including its format) during the whole incident management process;

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

h) identifying lessons learned, and any improvements to the plan and/or security in general that are required;

i) making those identified improvements.

Planning and preparation of the incident response 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 part of ISO/IEC 27035 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 IRT members and partner organizations. This includes names and identifiers for organizations and teams, information assets, business processes, etc. 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 involved 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.

Involved 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.

© ISO/IEC 2016 – All rights reserved

6.3 Involved 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 members of the PoC (Point of Contact), the IRT, management, public relations personnel and legal representatives);

c) reporting information security vulnerabilities (this is the responsibility of any permanent or contracted personnel in an organization and its companies) and dealing with them.

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

If involved 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 be 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 of instances like this are when the organization is using cloud system run by the third party or when third party is performing digital forensics for the organization or when working 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 considers specific incident types and the corresponding response processes. 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 be associated with 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 impacts on the organization's business operations, and associated guidance.

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

   2) An information security database 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 database will 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.

 © ISO/IEC 2016 – All rights reserved

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, anyone assessing an information security event, incident or vulnerability 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 could evolve to a significant or a crisis situation if not handled properly or a minor information security incident not followed up in a week could become a major information security incident.

4) Procedures to be followed to ensure that all information security incident management 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 vulnerability tracking and information security report updates, and updates to the plan itself.

6) Procedures for information security evidence analysis.

7) 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.

8) Guidance and procedures associated with the technical and organizational 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.

9) Material for the information security event, incident and vulnerability management awareness and training program.

10) Procedures and specifications for the testing of the information security incident management plan.

11) The plan of organizational structure for information security incident management.

12) The terms of reference and responsibilities of the IRT as a whole, and of individual members.

13) Important contact information.

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

b) Detection and reporting.

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 incident 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, and 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 policy, and assignment of technical and management roles. The format of reports and notification should match the incident classification scale or a consistent related metric.

© ISO/IEC 2016 – All rights reserved

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

5) Responding to incorrect use of the reporting process (potentially including taking action outside the scope of the incident management plan).

6) Collecting the information on information security events.

7) Detecting and reporting on information security vulnerabilities.

8) Recording information gathered in the information security database.

c) Assessment and decision.

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 assessment and decision 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 will allow response planners to develop consistent processes for completeness and classification of detected and reported events. The information sufficiency 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.

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. The incident handling process owner should ensure an information security database is sufficiently defined prior to developing the response processes that depend on it.

4) The PoC 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.

5) The IRT assessing information security events should confirm whether an event is an information security incident or not. To do this, another assessment 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 decisions being made on how the confirmed information security incident should be dealt with, by whom and in what priority, as well as escalation levels.

6) Assessing information security vulnerabilities (that have not yet been exploited to cause information security events and potential information security incidents), with decisions made on which need to be dealt with, by whom, how and in what priority.

7) Fully recording all assessment results and related decisions in the information security database.

d) Responses.

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 handling process owner should gather definitions or create working thresholds or categories for 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 assessment and decision preparations, and enable the IRT manager to assign the incident actions or tasks to responders.

© ISO/IEC 2016 – All rights reserved

2) Classes 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 reported and assessed incident. Immediate or deferred response should be included, as well as a definition of how single or cyclic incident tasks will be managed in the response process.

3) Review by the IRT to determine if the information security incident is under control,

   i) if the incident is under control, instigate the required response, either immediately (in real-time or in near real-time) or at a later time, and

   ii) if the incident is not under control or it is going to have a severe impact on the organization's core services, instigate crisis activities through escalation to crisis handling function.

4) Defining a map of all internal and external functions and organizations that should be involved during the management of an incident.

5) Containing and eradicating the information security incident as appropriate to mitigate or prevent the scope and impact of the incident from increasing.

6) Conducting information security evidence analysis, as required.

7) Escalation, as required.

8) Ensuring that all involved activities are properly logged for later analysis.

9) Ensuring that electronic evidence is identified, collected/acquired and preserved.

10) Ensuring that the change control regime is maintained and thus that the information security database is kept up-to-date.

11) Communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations.

12) Dealing with information security vulnerabilities.

13) Once the incident has been successfully dealt with, formally closing it and recording this in the information security database.

14) Post-incident activity should include further analysis as required.

e) 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 impacts on business operations; both short and longer-term (for example, a significant disruption could occur sometime after an initial information security incident). Further, it should allow for some responses necessary for information security incidents that are completely unforeseen, where ad hoc controls are required. Even for this situation, organizations should encompass general guidelines in the plan documentation on the steps that can be necessary.

f) Lessons learned.

   1) Identifying the lessons learned from information security incidents and vulnerabilities.

   2) Reviewing, identifying and making improvements to information security control implementation (new and/or updated controls), as well as information security incident management policy, as result of the lessons learned.

   3) Reviewing, identifying and if possible, making improvements to the organization's existing information security risk assessment and management review results, as a result of the lessons learned.

© ISO/IEC 2016 – All rights reserved

4) Reviewing how effective the processes, procedures, the reporting formats and/or the organizational structure were in responding to assessing and recovering from each information security incident and dealing with information security vulnerabilities, and on the basis of the lessons learned identifying and making improvements to the information security incident management plan and its documentation.

5) Updating the information security database.

6) 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 impacts on the organization's business operations.

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

6.6 Incident forms

Incident forms, if used, should be created before they are needed. The number, type and format of the forms should be determined by the IRT and revised periodically to ensure their relevance. An additional form type that allows for descriptive text should exist. Its purpose is to provide mechanism to capture information in instances where existing forms are not sufficient or an appropriate form has not yet been created.

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.

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 could 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 Processes and procedures

NOTE For brevity purposes, the term "document" will be used to refer to both processes and procedures in this text unless the distinction between a process and procedure is significant.

Before being able to commence 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.

It is important to understand that not all documents need to 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 IRT in order to interact with it. The IRT 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 and if 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 a bank employee who is embezzling funds is aware of some details how the investigation is being done, he or she can be able to better hide their activities from investigators or otherwise hamper the detection, investigation of and recovery from an information security incident.

 © ISO/IEC 2016 – All rights reserved

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 might be involved and their environment. Thus, an operating procedure could be related to a particular type of incident or product (for example, firewalls, databases, operating systems, applications) or to a specific 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.

There should be operating procedures for dealing with types of information security events and incidents that are already known, as well as vulnerabilities. There should also be operating procedures to be followed when an identified information security event, incident or 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) pre-authorized delegation of decision making without normal approval process.

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 (an individual may be allocated more than one role, depending on the size, structure and business nature of an organization), for example, including the following:

— 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 and crisis management procedures and actions in line with the system, service and/or network security policy;

— monitoring and maintain 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 and other relevant parties. All contacts and communications with outside parties should be documented for liability and evidentiary purposes.

6.8 Trust and confidence

The IRT plays a crucial role for the overall information security of an organization. The IRT requires the collaboration of all organizational personnel to detect, resolve and investigate information security incidents. It is fundamental that the IRT is trusted by the whole organization and that external entities have confidence in it. The trust within the organization is created by fiat and stems from the support given by the top management, i.e. the trust is given. External entities that have to deal with the IRT (e.g. IRTs from other organizations) need to be confident that the IRT will perform its job professionally, i.e. the trust should be earned.

The IRT can earn trust through transparency and mature processes. The IRT should work to educate users (internal and external), explain how the IRT works, how it protects confidentiality of information collected and how it manages security event, incident and vulnerability reports. The IRT 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.

© ISO/IEC 2016 – All rights reserved

The IRT 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 IRT should also be independently audited to confirm that all business requirements are being satisfied effectively.

Further, 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 anonymize sensitive information when required (e.g. when leaving the protective domain of the IRT). 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 omitted. Give that the IRT would still have to have access to the omitted information, this can lead to a situation where the IRT will maintain its own information security database.

As outlined elsewhere in this part of ISO/IEC 27035, 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, and the general public.

7 Establishing an incident response team (IRT)

7.1 General

NOTE Clause 7, in its entirety, links to ISO/IEC 27035-1:2016, 5.2 d).

The aim of establishing the IRT 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. An IRT contributes to the reduction in physical and monetary damage, as well as the reduction of the damage to the organization's reputation that is sometimes associated with information security incidents.

IRTs can be structured differently depending on the organization size, its staff members and industry type.

7.2 IRT types and roles

An IRT should have a defined constituency for which it is primarily responsible. Constituencies may be defined in many different ways including (but not limited to) employees of an organization, being assigned a specific IP address range, belonging to a specific autonomous system (AS) in IP routing, belonging to a specific domain (e.g. example.org), having customers of a product, having customers of a commercial incident response service, or covering the population of a region or country. Members may join the constituency voluntarily, as the result of contractual agreement (e.g. the purchase of a service or product) or by legislation (e.g. the establishment of a national CERT).

The characteristics and size of the constituency and the level of authority and control the IRT has over its members, will affect 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).

 © ISO/IEC 2016 – All rights reserved

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

Although the primary role of an IRT is to respond to incidents (whether detected by its own monitoring systems, reported from within the constituency, or reported by external sources), many teams also contribute a preventive role by improving security standards and practice within their constituencies, so as to reduce the likelihood and/or severity of incidents. IRTs are also likely to have an administrative role, for example, in reporting and managing their own policies, processes and resources.

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 types. 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.

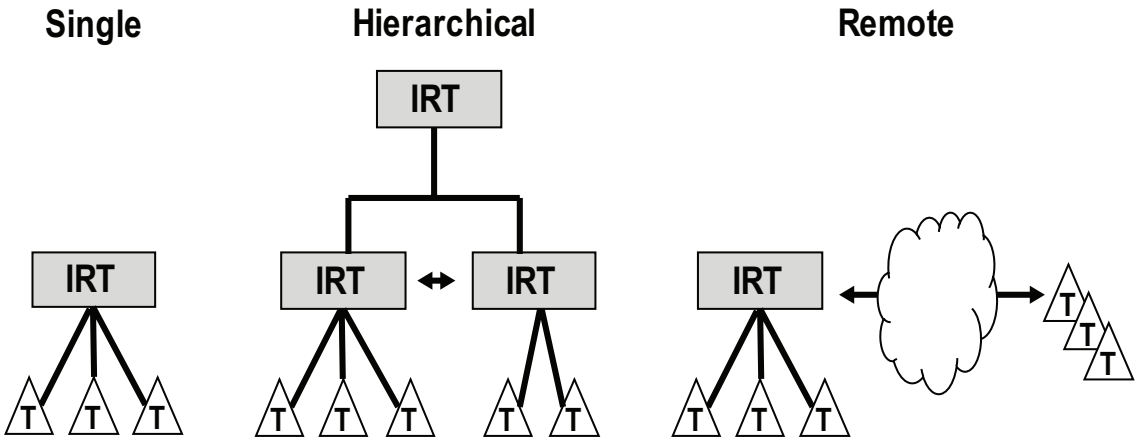

Figure 1 — Example IRT structures

— 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.

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

— *Managing Integrated security systems*: Monitoring and information security event management of 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*: Reacting quickly to threats, breaches, and attacks to minimize damage and reduce cost of recovery..

© ISO/IEC 2016 – All rights reserved

Duties of an IRT may also include monitoring and management activities as follows:

— *Integrated management and monitoring*: 24 × 7 × 365 h monitoring of targets, proactive monitoring and responses against incidents, logs management.

— *Reports management*: Periodic security reporting, security patches 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 IRT.

7.3 IRT staff

Effective incident response depends on the capability and reliability of IRT staff members. IRT staff and their capabilities become even more important when the activities of IRTs include establishing security incident management policy, auditing, coordinating with other departments, and advancing technical activities. 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, programming.

In order to respond to various types of incidents, IRT members should possess technical knowledge and skills such as the following:

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

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

— cryptography (encryption and hash algorithms), digital signatures, current protocols such as SSL/TLS;

— common network protocols such as ethernet (IEEE 802.3), WiFi (IEEE 802.11) IPv4, IPv6, ICMP, UDP, TCP;

— common network application protocols such as DNS, 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 part of ISO/IEC 27035 was developed. IRT members should maintain current knowledge and skills.

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

 © ISO/IEC 2016 – All rights reserved

Table 1 — Example roles and tasks of IRT staff members

Role	Description
IRT Manager	The leadership role is responsible for managing the staff members, defining the job scope, and reporting the status to higher-level organizations.
Planning	Responsible for operating an IRT. It establishes or plans various security policies, reports them to higher-level authorities, cooperates with third parties, and register and approve vulnerability reports. Its roles are as follows: a) establishing and planning security policies; b) implementing security processes; c) adjusting the risk priorities; d) communicating with higher-level organizations and other third-party organizations; e) supporting administration; f) discussing/registering/approving vulnerability reports on the target organizations; g) performing other activities directed by the IRT manager.
Monitoring	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 h monitoring and operation; b) intrusion trial detection, registering incidents, and first responses; c) performing the security patches and upgrades; d) implementation of the security policy and backup management; e) help desk; f) facility management; g) performing other activities directed by the IRT manager.
Response	Manages the case from the monitoring agents for incidents related to intrusion to for incidents related to intrusion, theft, data exfiltration or exposure, performs secondary further analysis and actions including investigation efforts, performs recovery actions and establishes adequate strategy. Services such as real-time responses, technical support, and the following are also provided: a) propagating and reporting incidents; b) correlation analysis between monitoring systems; c) incident investigation and recovery supports; d) vulnerability analysis on the target organization and IRT; e) performing other activities directed by the IRT manager.
Analysis	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 IRT manager.

© ISO/IEC 2016 – All rights reserved

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

Table 2 — Example IRT staff positions

Staff title	Tasks
Manager or team lead	— provides strategic direction — enables and facilitates work of team members — supervises team — represents IRT to management and others — interviews and hires new team members
Assistant managers, supervisors, or group leaders	— supports strategic direction of assigned functional area — supports the team lead as needed — provides direction and mentoring to team members — assigns tasks and duties — participates in interviews with new team members
Help desk or triage staff	— handle main IRT telephone(s) for incident or security reports — provide initial assistance, depending on skills — undertake initial data entry and the sorting and prioritizing of incoming information
Incident handlers	— undertake incident analysis, tracking, recording, and response — coordinate the reactive and proactive guidance that will be provided to the constituency (develop material such as documentation, checklists, best practices, and guidelines) — disseminate information — interact with the IRT team, external experts, and others (such as sites, media, law enforcement, or legal personnel) as appropriate, by assignment from team lead or other management staff — 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 with new staff members as directed
Vulnerability handlers	— analyse, test, track and record vulnerability reports and vulnerability artefacts — research or develop patches and fixes as part of the vulnerability response effort — interact with the constituency, the IRT team, software application developers, external experts (other IRTs, researchers, vendors) and others (media, law enforcement, or legal personnel), as required — disseminate information on vulnerabilities and corresponding fixes, patches, or workarounds — undertake technology-watch activities, if assigned — mentor new IRT staff, as assigned — participate in interviews with new IRT staff
Technical writers	— assist and facilitate the IRT in the development of publications such as advisories, best practices, or technical tips

© ISO/IEC 2016 – All rights reserved

8 Establishing relationships with other organizations

8.1 General

NOTE Clause 8, in its entirety, links to ISO/IEC 27035-1:2016, 5.2 e).

It is necessary 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 need to understand what the IRT is and how it can help support their business processes. Agreements should be made concerning the IRT's authority over business systems and who will make decisions if critical business systems need to be disconnected from the network or shut down.

— **Representatives from IT**. The interactions and workflow between the IT staff and the IRT should be defined including what actions will be taken by IT staff and what actions are taken by IRT members, hat information the IT staff can provide to the IRT and what information the IRT can provide to the IT team, and what roles 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.

— **Representatives from human resources**. They will need to be involved in developing policies and procedures for removing 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**. The IRT will need to exchange information with these groups about computer incidents and may share responsibility with them for resolving issues involving computer or data 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 will understand how the team should work with law enforcement, when to contact law enforcement and who will do the investigations and forensic analysis.

— **General representatives from the constituency**. They can provide insight into their needs and requirements.

The IRT should have the responsibility for ensuring that incidents are resolved and in this context, the IRT manager and members of the team 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 details the appropriate authority to which the IRT manager reports serious information security incidents. The authority, on its part, should make commitment to make itself available to IRT members and deliver its guidance in a timely fashion.

© ISO/IEC 2016 – All rights reserved

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 IRT. All IRT members should be taught how to refer media questions according to the media policy.

8.3 Relationship with external interested parties

Organizations should establish relationships between the IRT and appropriate external interested parties. IRTs often need to communicate with outside parties regarding an incident and they should do so whenever appropriate, such as contacting law enforcement, fielding media inquiries, and seeking external expertise. Another example is discussing incidents with other involved parties, such as Internet Service Providers (ISPs), the vendor of vulnerable software or other IRTs. 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 IRT policies and processes and according to any legal or legislative regulations.

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 detection and reporting 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) external organizations' IRTs;

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

d) law enforcement organizations;

e) emergency authorities;

f) appropriate government organizations;

g) legal personnel;

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

i) business partners;

j) customers;

k) general public.

9 Defining technical and other support

9.1 General

NOTE Clause 9, in its entirety, links to ISO/IEC 27035-1:2016, 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

 © ISO/IEC 2016 – All rights reserved

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;

— access to the documented procedures related to crisis management;

— 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 database and the technical means to populate and update the database quickly, analyse its information and facilitate responses (in some instances manual records can be required by an organization), with the database 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;

— facilities for information security/digital evidence collection and analysis;

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

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

An organization should ensure that the technical means used to populate and update the database quickly, analyse its information and facilitate responses to information security incidents support the following:

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

b) notification of previously selected external personnel by appropriate means (for example, electronic mail, fax or telephone), thus requiring the maintenance of a reliable, readily accessible contact database (including paper and other backups), and the facility 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 data about the information system, service and/or network, and all data 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 off-line storage in read-only media such as CD or DVD ROM);

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

    1) backup testing;

© ISO/IEC 2016 – All rights reserved

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.

Organizations can create a standard baseline image from the installation media and use that image 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 Technical means described in 9.1 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 Examples of technical support

Such mechanisms could 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 watch 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 ISO/IEC 27033);

f) anti-malicious code software;

g) audit log records, and log monitoring software.

9.3 Examples of other support

Such mechanisms could include documented responsibilities and operating procedures for the operations support team.

10 Creating information security incident awareness and training

NOTE Clause 10, in its entirety, links to ISO/IEC 27035-1:2016, 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 27001:2013, 7.2).

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. Further, the operational efficiency and quality of a structured approach to information

 © ISO/IEC 2016 – All rights reserved

security incident management relies on a number of factors, including obligation to notify stakeholders 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 corporate information security awareness and training program. The awareness program 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 program or programs 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 database;

e) controls on confidentiality of sources as relevant;

f) plan service level agreements;

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

h) any constraints imposed by non-disclosure agreements;

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

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

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

© ISO/IEC 2016 – All rights reserved

11 Testing the information security incident management plan

11.1 General

NOTE Clause 11, in its entirety, links to ISO/IEC 27035-1:2016, 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 vulnerabilities. Periodic tests should be organized to check processes/procedures and to verify the IRT 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 will depend 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 might 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.

The main types of exercises are as follows:

— discussion-based;

— tabletop;

— live;

— combination of the above.

Which type of the exercise will be used depends on the goal that wants to be achieved but also available time and resources.

Every exercise goes through the following phases:

— planning and preparation;

— execution;

— debrief and post-mortem analysis.

Planning and preparation of an exercise is based on the current incident response plans and envisaged future threats and trends. The results of the post-mortem analysis are used as input to improvement of the incident response 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 response plans and identify potential omissions;

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.

 © ISO/IEC 2016 – All rights reserved

It is common that an exercise have 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 response plans or updating the existing ones, it can use exercises to validate them. After the plans were made and put in place, the organization will use exercises to train the people. After the existing processes and procedures are well established, they need to be periodically tested to ensure that they are still valid.

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

Table 3 — Mapping exercise goals to the exercise types

Goal	Type of an exercise
Validating new plans	discussion-based tabletop
Training people	discussion-based tabletop live
Verifying if the existing plans are still valid	tabletop 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 need to be considered:

a) is the exercise only for internal people (within the organization) or external organization will be involved;

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

c) how many exercise leaders are required.

The scope has direct influence on which organizations will be 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 will 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 need to 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 sufficient number of people are available to lead participants through the exercise;

e) sufficient time should be allocated to discussion during the exercise but not excessive amount to derail the exercise;

© ISO/IEC 2016 – All rights reserved

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

g) create and distribute exercise reports to the stakeholders.

11.3 Incident response capability monitoring

11.3.1 Implementing an incident response capability monitoring program

Incident response capabilities encompass not only capabilities of the IRT but also capabilities of individuals and groups that IRT may ask for help during the incident handling. While most of the incident response capabilities will be 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 who can 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 need to possess. These capabilities will change over time. Some changes will happen because technology within the organization will change by either abandoning it or introducing a new one. An example of the abandoning a technology might 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 existed within the organization. Another reason that can require change in the IRT capabilities is 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 required that it 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 organization current capabilities. The following non-exhaustive list illustrates what information can be contained in this register:

a) what capabilities are available to the organization;

b) who possesses them;

c) are they internal or external to the organization;

d) how to engage the bearer of the capability;

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

f) 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 could be gained and so on.

© ISO/IEC 2016 – All rights reserved

12 Lessons learned

12.1 General

NOTE Clause 12, in its entirety, links to ISO/IEC 27035-1:2016, 5.6.

Once an information security incident has been closed, it is important that the organization should quickly identify and learn from the lessons after handling an information security incident and ensure that the conclusions are acted upon. Further, there could be lessons to be learned from the assessment and resolution of reported information security vulnerabilities. The lessons learned can result in one or more of the following outcomes.

a) New or changed requirements for information security controls. These could be technical or non-technical (including physical) controls. Dependent on the lessons learned, these could 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.

b) New or changed threat and vulnerability information and thus changes to the organization's existing information security risk assessment and management review results.

c) Changes to the information security incident management plan and its processes, procedures, the reporting formats and/or the organizational structure, and the information security database.

12.2 Identifying the lessons learned

An organization should look beyond a single information security incident or vulnerability and check for trends/patterns which themselves may help identify the need for controls or approach 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 database on a regular basis in order to do the following:

— identify trends/patterns;

— identify areas of concern;

— analyse where preventive action could 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 what further information security incidents could arise, based on previous experience and documented knowledge.

Use should also be made of information security incident and related vulnerability information received from government, other IRTs and suppliers.

Vulnerability assessment/security testing of an information system, service and/or network following an information security incident, should not be confined to only the information system, service and/or network, affected by the information security incident. It should be expanded to include any related information systems, services and/or networks. A complete vulnerability assessment is used to highlight the existence of the vulnerabilities exploited during the information security incident on other information systems, services and/or networks and to ensure that no new vulnerabilities are introduced.

It is important to stress that vulnerability assessments should be conducted on a regular basis and that the re-assessment of vulnerabilities after an information security incident has occurred should be part of this continuous assessment process and not as a replacement.

© ISO/IEC 2016 – All rights reserved

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.

12.3 Identifying and making improvements to information security control implementation

During review, after one or more information security incidents or 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 needs to 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 could 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. Further, an organization's information systems, services and/or networks should be subject to regular vulnerability assessments to aid in the identification of vulnerabilities and provide a process of continual system/service/network hardening.

In addition, while reviews of information security-related procedures and documentation can be conducted in the immediate aftermath of an information security incident or a resolved vulnerability, it is more likely that this is required as a later response. Following an information security incident or a resolved vulnerability, if relevant, an organization should update its information security policies and procedures to take into account information gleaned and any problem issues identified during the course of the incident management process. It should be a long-term aim of the IRT, 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 lessons learned phase, for example, changes in information security policies, standards and procedures, and changes to IT hardware and software configurations. The organization should ensure that these are acted upon.

A special case of lessons learned is the analysis of 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. Potential result of this analysis can be to highlight deficiencies in other, non-security related processes or parts of the organization, to the top management.

12.4 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 related to a reported information security vulnerability), an assessment of information security risk assessment and management review results could be necessary to take into account new threats and vulnerabilities. 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).

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

As a part of post-incident resolution, the IRT manager or a nominee should review all that has happened to assess and thus quantify the effectiveness of the entire response to an information security incident.

© ISO/IEC 2016 – All rights reserved

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 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.

12.6 IRT evaluation

Compared to lessons learned, an evaluation is a periodic and more holistic assessment of the effectiveness of the IRT. Once the IRT 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 lessons learned processes.

Examples of evaluation activities include the following:

— determining which activities work well and which do not.

— revising policies and design and implementation plans as appropriate.

— evaluating the capabilities and services once they become operational.

— checking how the IRT 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 IRT.

Performance metrics can also be collected to help evaluate IRT 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;

© ISO/IEC 2016 – All rights reserved

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

— preventative techniques and security practices in place.

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

12.7 Other improvements

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

— overly long time or infrequent production of remedies can lead to refining criteria for selecting software or hardware vendor;

— insufficient staffing during handling of the incident can improve scheduling of absence from the work;

— lack of knowledge can point to gaps in education.

© ISO/IEC 2016 – All rights reserved

Annex A
(informative)

Legal and regulatory aspects

The following legal and regulatory aspects of information security incident management should be addressed in the information security incident management policy and associated scheme.

a) **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 need to be typically attributed to an individual, information of a personal nature may therefore need to be recorded and managed accordingly. A structured approach to information security incident management therefore needs to take into account the appropriate privacy protection. This may include the following:

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

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

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

b) **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).

c) **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, an organization should ensure 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 should be ensured that all requirements, including response times, are included in the contract with the external party.

d) **Legal issues related to policies and procedures are dealt with**. The policies and procedures associated with the information security incident management scheme should be checked for potential legal and regulatory issues, for example if there are statements about disciplinary and/or legal action taken against those causing information security incidents. In some countries, it not easy to terminate employment.

e) **Disclaimers are checked for legal validity**. All disclaimers regarding actions taken by the information incident management team and any external support personnel, should be checked for legal validity.

f) **Contracts with external support personnel cover all required aspects**. Contracts with any external support personnel, for example from an external IRT, should be thoroughly checked regarding waivers on liability, non-disclosure, service availability, and the implications of incorrect advice.

© ISO/IEC 2016 – All rights reserved

g) **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; this should be checked.

h) **Law enforcement requirements are addressed**. The issues associated with the possibility that law enforcement agencies might legally request information from an information security incident management scheme need to be clear. It may be the case that clarity is required on the minimum level required by law at which incidents should be documented and how long that documentation should be retained.

i) **Liability aspects are clear.** The issues of potential liability and related required controls to be in place need to be clarified. Examples of events which may have associated liability issues are as follows:

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

   2) 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 on one or more other organizations;

   3) 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;

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

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

j) **Specific regulatory requirements are addressed**. Where required by specific regulatory requirements, incidents should be reported to a designated body, for example as required in the nuclear power industry, Telecommunications companies and Internet Service Providers in many countries.

k) **Prosecutions, or internal disciplinary procedures, can be successful**. The appropriate information security controls should be 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, evidence will typically need to be 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

   1) records are complete and have not been tampered with in any way,

   2) copies of electronic evidence are provably identical to the originals, and

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

l) **Legal aspects associated with monitoring techniques are addressed.** The implications of using monitoring techniques need to be addressed in the context of the relevant national legislation. The legality of different techniques will vary from country to country. For example, in some countries, it is necessary to make people aware that monitoring of activities, including through surveillance techniques, takes place. Factors that need to be considered include who/what is being monitored, how they/it are being monitored, and when the monitoring is occurring. It should also be noted that monitoring/surveillance in the context of IDS is specifically discussed in ISO/IEC 27039.

© ISO/IEC 2016 – All rights reserved

m) **Acceptable use policy is defined and communicated.** Acceptable practice/use within the organization should be defined, documented and communicated to all intended users. For example, users should be 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.

© ISO/IEC 2016 – All rights reserved