ISO/IEC JTC 1/SC 27 N15987

REPLACES: N15796

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: text for FDIS ballot

TITLE: **Text for ISO/IEC FDIS 27035-1:2016-02-15(E), Information technology – Security techniques – Information security incident management — Part 1: Principles of incident management**

SOURCE: **ITTF**

DATE: 2016-02-25

PROJECT: **1.27.71.01 (ISO/IEC 27035-1, revision of 27035)**

STATUS: **This document is currently undergoing a 2-month FDIS letter ballot at the JTC 1 level. The P-members of JTC 1 and SC 27 are kindly requested to submit their votes on ISO/IEC FDIS 27035-1:2016-02-15(E) directly to the ISO Central Secretariat via the ISO e-balloting application by 2016-04-15. It is circulated within SC 27 for information.**

ACTION: **ITTF**

DUE DATE: **2016-04-15**

DISTRIBUTION: P-, O- and L-Members
L. Rajchel, JTC 1 Secretariat
H. Cuschieri, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice Chair
E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors
Jinghua Min, Art Manion, Geoff Clark, Project co-editors

MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

NO. OF PAGES: 1 + 32 + 17 (attachment 1)

FINAL
DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 27035-1

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on: **2016-02-15**

Voting terminates on: **2016-04-15**

Information technology — Security techniques — Information security incident management —

Part 1: **Principles of incident management**

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

Partie 1: Principes de la gestion des incidents

Reference number
ISO/IEC FDIS 27035-1:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27035-1, together with ISO/IEC 27035-2 and ISO/IEC TS 27035-3, cancels and replaces ISO/IEC 27035:2011, which has been technically revised.

ISO/IEC 27035 consists of the following parts, under the general title *Information technology — Security techniques — Information security incident management*:

— *Part 1: Principles of incident management*

— *Part 2: Guidelines to plan and prepare for incident response*

The following parts are under preparation:

— *Part 3: Guidelines for CSIRT operations* [Technical Specification]

Introduction

About this International Standard

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

- detect, report and assess information security incidents;
- respond to information security incidents, including the activation of appropriate controls to prevent, reduce, and recover from impacts;
- report information security vulnerabilities, so they can be assessed and dealt with appropriately;
- learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management.

For the purpose of achieving this planned approach, ISO/IEC 27035 provides guidance on aspects of information security incident management in the following corresponding parts.

- ISO/IEC 27035-1, *Principles of incident management* (this International Standard), presents basic concepts and phases of information security incident management, and how to improve incident management. This part combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.
- ISO/IEC 27035-2, *Guidelines to plan and prepare for incident response*, describes how to plan and prepare for incident response. This part covers the "Plan and Prepare" and "Lessons Learnt" phases of the model presented in ISO/IEC 27035-1.
- ISO/IEC TS 27035-3, *Guidelines for CSIRT operations*, describes the activities associated with the Detection and Reporting, Assessment and Decision, and Response (including Post Incident Activity) phases of the model presented in ISO/IEC 27035-1.

Relationship to other standards

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

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

This International Standard also intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

Further information about investigative standards is available in Annex A.

Information technology — Security techniques — Information security incident management —

Part 1: Principles of incident management

1 Scope

This part of ISO/IEC 27035 is the foundation of this multipart International Standard. It presents basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.

The principles given in this part of ISO/IEC 27035 are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this part of ISO/IEC 27035 according to their type, size and nature of business in relation to the information security risk situation. This part of ISO/IEC 27035 is also applicable to external organizations providing information security incident management services.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27035-2,[1]*Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

ISO/IEC/TS 27035-3,[2]*Information technology — Security techniques — Information security incident management — Part 3: Guidelines for CSIRT operations*

3 Terms and definitions

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

3.1
information security investigation
application of examinations, analysis and interpretation to aid understanding of an *information security incident* (3.4)

[SOURCE: ISO/IEC 27042, 3.10, modified — The phrase “an incident” was replaced by “an information security incident”.]

[1] To be published.

[2] Under preparation.

3.2
Incident Response Team
IRT
team of appropriately skilled and trusted members of the organization that handles incidents during their lifecycle

Note 1 to entry: CERT (Computer Emergency Response Team) and CSIRT (Computer Security Incident Response Team) are commonly used terms for IRT.

3.3
information security event
occurrence indicating a possible breach of information security or failure of controls

3.4
information security incident
one or multiple related and identified *information security events* (3.3) that can harm an organization's assets or compromise its operations

3.5
information security incident management
exercise of a consistent and effective approach to the handling of *information security incidents* (3.4)

3.6
incident handling
actions of detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (3.4)

3.7
incident response
actions taken to mitigate or resolve an *information security incident* (3.4), including those taken to protect and restore the normal operational conditions of an information system and the information stored in it

3.8
Point of Contact
PoC
defined organizational function or role serving as the coordinator or focal point of information concerning incident management activities

4 Overview

4.1 Basic concepts and principles

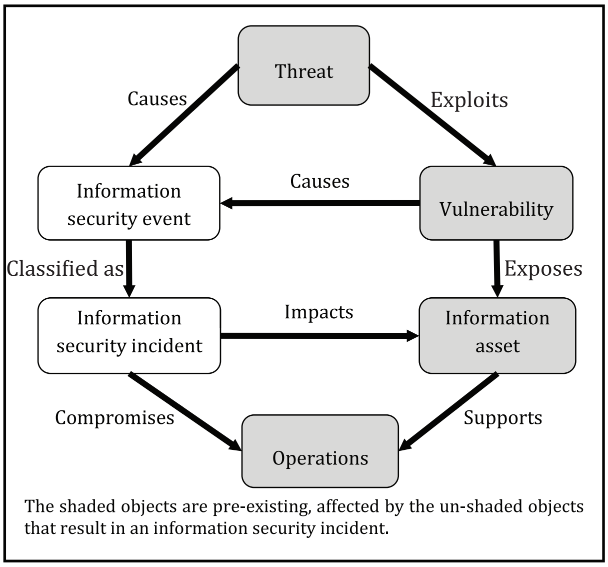
An information security event is an occurrence indicating a possible breach of information security or failure of controls. An information security incident is one or multiple related and identified information security events that meet established criteria and can harm an organization's assets or compromise its operations.

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

Information security incidents can be deliberate (e.g. caused by malware or intentional breach of discipline) or accidental (e.g. caused by inadvertent human error or unavoidable acts of nature) and can be caused by technical (e.g. computer viruses) or non-technical (e.g. loss or theft of computers) means. Consequences can include the unauthorized disclosure, modification, destruction, or unavailability of information, or the damage or theft of organizational assets that contain information.

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

A threat exploits vulnerabilities (weaknesses) in information systems, services, or networks, causing the occurrence of information security events and thus potentially causing incidents to information assets exposed by the vulnerabilities. Figure 1 shows the relationship of objects in an information security incident.



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

Figure 1 — Relationship of objects in an information security incident

Information sharing and coordination with external IRTs is an important consideration. Many incidents cross organizational boundaries and cannot be easily resolved by a single IRT. Information sharing and coordination relationships or partnerships with external IRTs can greatly enhance the ability to respond to and resolve incidents. For further detail about information sharing, see ISO/IEC 27010.

4.2 Objectives of incident management

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

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

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

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

c) the adverse effects of information security incidents on the organization and its operations are minimized by appropriate controls as part of incident response;

d) a link with relevant elements from crisis management and business continuity management through an escalation process is established;

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

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

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

Another objective associated with this part of ISO/IEC 27035 is to provide guidance to organizations that aim to meet the Information Security Management System (ISMS) requirements specified in ISO/IEC 27001 which are supported by guidance from ISO/IEC 27002. ISO/IEC 27001 includes requirements related to information security incident management. A table that cross-references information security incident management clauses in ISO/IEC 27001 and clauses in this part of ISO/IEC 27035 is provided in Annex C. ISMS relationships are also explained in Figure 2. This part of ISO/IEC 27035 can also support the requirements of information security management systems other than ISMS.

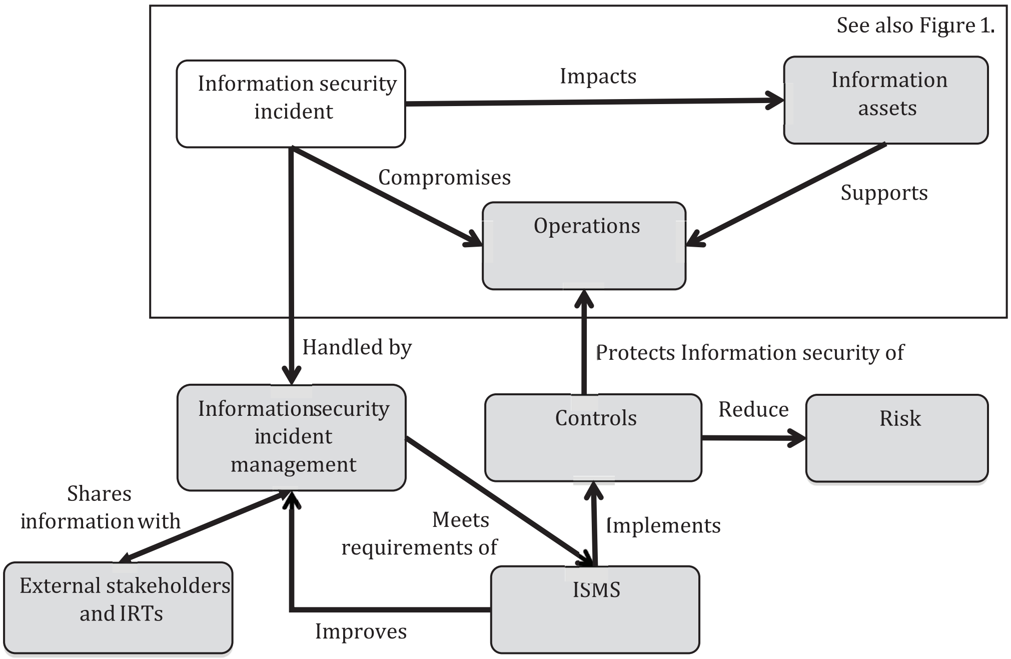


Figure 2 — Information Security Incident Management in relation to ISMS and applied controls

4.3 Benefits of a structured approach

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

a) Improving overall information security

A structured process for detection, reporting and assessment of and decision-making related to information security events and incidents will enable rapid identification and response. This will improve overall security by helping to quickly identify and implement a consistent solution, and thus provide a means of preventing future similar information security incidents. Furthermore, there will be benefits gained by metrics, sharing and aggregation. The credibility of the organization will be improved by the demonstration of its implementation of best practices with respect to information security incident management.

b) Reducing adverse business impacts

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

c) Strengthening the focus on information security incident prevention

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

d) Improving prioritization

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

e) Supporting evidence collection and investigation

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

f) Contributing to budget and resource justifications

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

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

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

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

- better collection of data for assisting in the identification and determination of the characteristics of the various threat types and associated vulnerabilities, and
- provision of data about frequencies of occurrence of the identified threat types.

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

h) Providing enhanced information security awareness and training program material

A structured approach to information security incident management will enable an organization to collect experience and knowledge of how the organization handles incidents, which will be valuable material for an information security awareness program. An awareness program that includes lessons learnt from real experience will help reduce mistakes or confusion in future information security incidents.

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

Data provided by an information security incident management plan could provide valuable input to reviews of the effectiveness and subsequent improvement of incident management security policies (and other related information security documents). This applies to topic-specific policies and other documents applicable both for organization-wide and for individual systems, services and networks.

4.4 Adaptability

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

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

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

c) potential risk due to incidents;

d) the goals of the business.

An organization using this part of ISO/IEC 27035 should therefore adopt its guidance in a manner that is relevant to the scale and characteristics of its business.

5 Phases

5.1 Overview

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

- Plan and Prepare (see 5.2);
- Detection and Reporting (see 5.3);
- Assessment and Decision (see 5.4);
- Responses (see 5.5);

— Lessons Learnt (see 5.6).

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

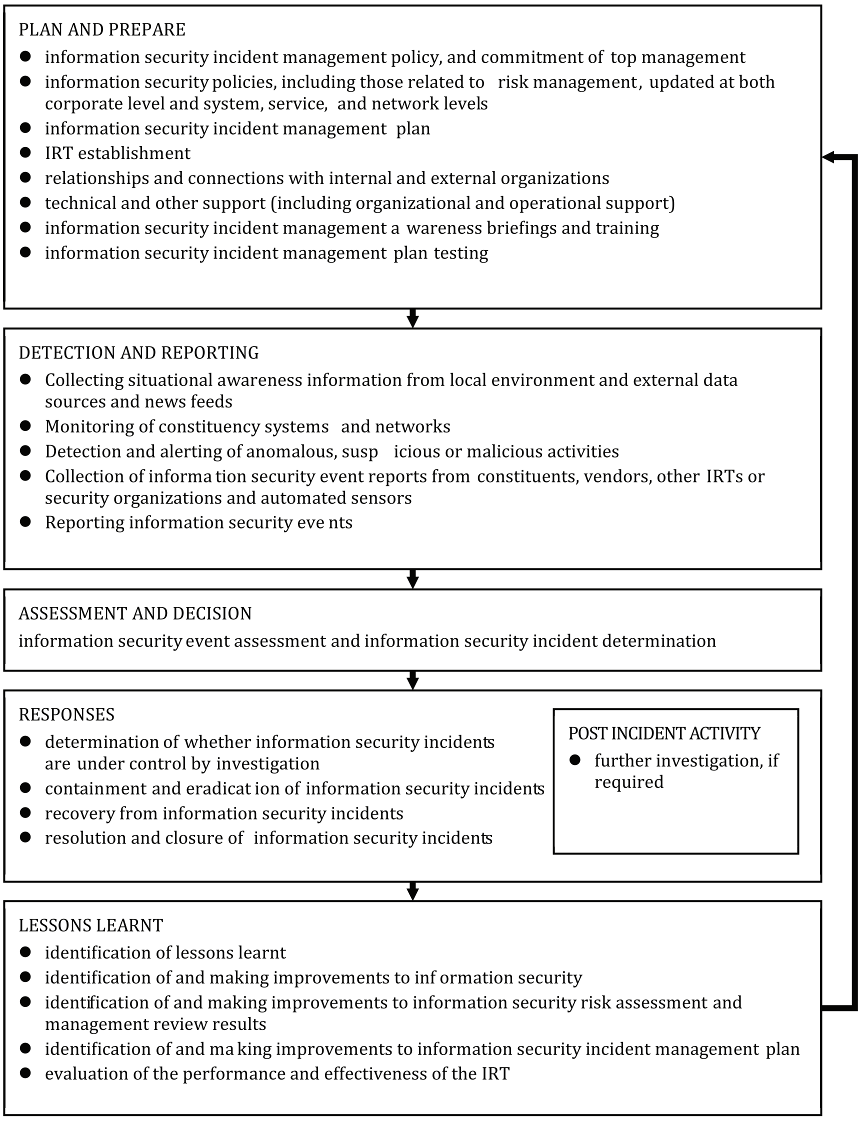
Some activities can occur in multiple phases or throughout the incident handling process. Such activities include the following:

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

— coordination and communication between the involved parties;

— notification of significant incidents to management and other stakeholders;

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



PLAN AND PREPARE

- information security incident management policy, and commitment of top management
- information security policies, including those related to risk management, updated at both corporate level and system, service, and network levels
- information security incident management plan
- IRT establishment
- relationships and connections with internal and external organizations
- technical and other support (including organizational and operational support)
- information security incident management awareness briefings and training
- information security incident management plan testing

DETECTION AND REPORTING

- Collecting situational awareness information from local environment and external data sources and news feeds
- Monitoring of constituency systems and networks
- Detection and alerting of anomalous, suspicious or malicious activities
- Collection of information security event reports from constituents, vendors, other IRTs or security organizations and automated sensors
- Reporting information security events

ASSESSMENT AND DECISION

information security event assessment and information security incident determination

RESPONSES

- determination of whether information security incidents are under control by investigation
- containment and eradication of information security incidents
- recovery from information security incidents
- resolution and closure of information security incidents

POST INCIDENT ACTIVITY

- further investigation, if required

LESSONS LEARNT

- identification of lessons learnt
- identification of and making improvements to information security
- identification of and making improvements to information security risk assessment and management review results
- identification of and making improvements to information security incident management plan
- evaluation of the performance and effectiveness of the IRT

Figure 3 — Information security incident management phases

As noted in the Introduction, ISO/IEC 27035 is in three parts.

- ISO/IEC 27035-1 covers all five phases.
- ISO/IEC 27035-2 covers
  - Plan and Prepare, and
  - Lessons Learnt
- ISO/IEC TS 27035-3 covers
  - Detection and Reporting,
  - Assessment and Decision, and
  - Responses (including Post Incident Activity).

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

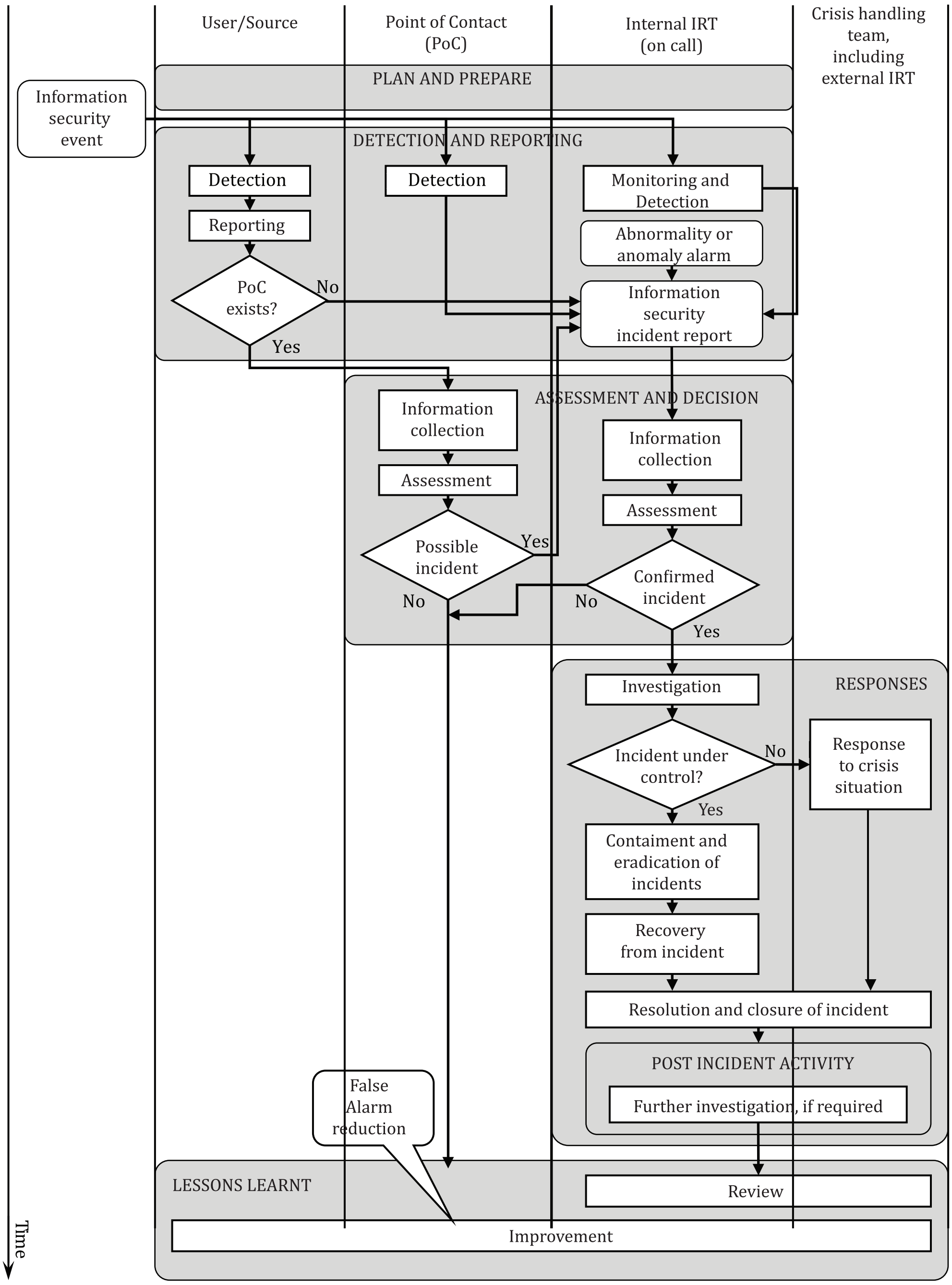


Figure 4 — Information security event and incident flow diagram

5.2 Plan and Prepare

Effective information security incident management requires appropriate planning and preparation. For an efficient and effective information security incident management plan to be put into operation, an organization should complete a number of preparatory activities, namely:

a) formulate and produce an information security incident management policy and gain top management commitment to that policy;

b) update information security policies, including those related to risk management, at a corporate level and specific system, service and network levels;

c) define and document a detailed information security incident management plan, including topics covering communications and information disclosure;

d) establish the IRT, with an appropriate training program designed, developed, and provided to its personnel;

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

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

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

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

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

5.3 Detection and Reporting

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

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

For the Detection and Reporting phase, an organization should undertake the following key activities:

a) monitor and log system and network activity of constituency or parent organizations as appropriate;

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

c) collect information on an information security event or vulnerability;

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

e) ensure that all activities, results and related decisions are properly logged for later analysis;

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

g) ensure that a change control regime is followed to enable information security event and vulnerability tracking and report updates, and to keep the information security database up-to-date;

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

All information collected pertaining to an information security event or vulnerability should be stored in the information security database managed by the IRT. The information reported during each activity should be as complete as possible at the time. This will support assessments, decisions and actions to be taken.

ISO/IEC TS 27035-3 describes in detail each of the activities listed above.

5.4 Assessment and Decision

The third phase of information security incident management involves the assessment of information associated with occurrences of information security events and the decision on whether to classify events as information security incidents.

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

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

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

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

For the Assessment and Decision phase, an organization should perform the following key activities:

- collect information that can include testing, measuring, and other data gathering about the detection of an information security event. The type and amount of information collected will depend on the information security event that has occurred;
- conduct an assessment by the incident handler to determine whether the event is a possible or confirmed information security incident or a false alarm. A false alarm (i.e. a false positive) is an indication of a reported event that is found not to be real or of any consequence. If desired, the IRT can conduct a quality review to ensure that the incident handler correctly declared an incident;
- ensure that all parties involved, particularly the IRT, properly log all activities, results and related decisions for later analysis;
- ensure that the change control regime is maintained to cover information security incident tracking and incident report updates, and to keep the information security database up-to-date.

All information collected pertaining to an information security event, incident or vulnerability should be stored in the information security database managed by the IRT. The information reported during each activity should be as complete as possible at the time. This will support assessments, decisions and actions to be taken.

ISO/IEC TS 27035-3 describes in detail each of the activities listed above.

5.5 Responses

The fourth phase of information security incident management involves responding to information security incidents in accordance with the actions determined in the Assessment and Decision phase. Depending on the decisions, the responses could be made immediately, in real-time, or in near real-time, and some responses could involve information security investigation.

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

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

b) provide formal procedures for each involved person to follow, including reviewing and amending the reports, re-assessing damage, and notifying the relevant personnel. Individual actions will depend on the type and severity of the incident;

c) use guidelines for thorough documentation of an information security incident and subsequent actions.

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

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

— review by the IRT to determine whether the information security incident is under control, and if so, perform the required response. If the incident is not under control or it is going to have a severe impact on the organization's operations, perform crisis response activities through escalation to the crisis handling function.

— assign internal resources and identify external resources in order to respond to an incident.

— escalate as needed throughout the phase for further assessments or decisions.

— ensure that all parties involved, particularly the IRT, properly log all activities for later analysis.

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

— ensure that the change control regime is maintained to cover information security incident tracking and incident report updates, and to keep the information security database up-to-date.

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

— after recovery from an incident, a Post Incident Activity should be initiated depending on the nature and severity of the incident. This activity includes

  — investigation of the information pertaining to the incident,

  — investigation of other relevant sources such as involved personnel, and

  — summarized report of the investigation findings;

— once the incident has been resolved, it should be closed according to the requirements of the IRT or parent organization and all stakeholders should be notified.

All information collected pertaining to an information security event, incident, or vulnerability should be stored in the information security database managed by the IRT. The information reported during each activity should be as complete as possible at the time. This will support assessments, decisions and actions to be taken, including potential further analysis.

ISO/IEC TS 27035-3 describes in detail each of the activities listed above.

5.6 Lessons Learnt

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

For the Lessons Learnt phase, an organization should perform the following key activities:

a) identify the lessons learnt from information security incidents and vulnerabilities;

b) review, identify and make improvements to information security control implementation (new or updated controls), as well as information security incident management policy. Lessons can come from one or many information security incidents or reported security vulnerabilities. Improvements are aided by metrics fed into the organization’s strategy on where to invest in information security controls;

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

d) review how effective the processes, procedures, reporting formats and organizational structure were in responding to, assessing and recovering from information security incidents and dealing with information security vulnerabilities. On the basis of the lessons learnt, identify and make improvements to the information security incident management plan and its documentation;

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

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

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

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

ISO/IEC 27035-2 describes in detail each of the activities listed above.

Annex A
(informative)

Relationship to investigative standards

This part of ISO/IEC 27035 describes part of a comprehensive investigative process which includes, but is not limited to, the application of the following standards:

— ISO/IEC 27037, *Guidelines for the identification, collection, acquisition and preservation of digital evidence*

This describes the means by which those involved in the early stages of an investigation, including initial response, can ensure that sufficient potential digital evidence is captured to allow the investigation to proceed appropriately.

— ISO/IEC 27038, *Specification for digital redaction*

Some documents can contain information that should not be disclosed to some communities. Modified documents can be released to these communities after an appropriate processing of the original document. The process of removing information that is not to be disclosed is called “redaction”.

The digital redaction of documents is a relatively new area of document management practice, raising unique issues and potential risks. Where digital documents are redacted, removed information should not be recoverable. Hence, care needs to be taken so that redacted information is permanently removed from the digital document (e.g. it should not be simply hidden within non-displayable portions of the document).

ISO/IEC 27038 specifies methods for digital redaction of digital documents. It also specifies requirements for software that can be used for redaction.

— ISO/IEC 27040, *Storage security*

ISO/IEC 27040 provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.

Security mechanisms like encryption and sanitization can affect one’s ability to investigate by introducing obfuscation mechanisms. They should be considered prior to and during the conduct of an investigation. They can also be important in ensuring that storage of evidential material during and after an investigation is adequately prepared and secured.

— ISO/IEC 27041, *Guidance on assuring the suitability and adequacy of incident investigation methods*

It is important that methods and processes deployed during an investigation can be shown to be appropriate. This document provides guidance on how to provide assurance that methods and processes meet the requirements of the investigation and have been appropriately tested.

— ISO/IEC 27042, *Guidelines for the analysis and interpretation of digital evidence*

This describes how methods and processes to be used during an investigation can be designed and implemented in order to allow correct evaluation of potential digital evidence, interpretation of digital evidence and effective reporting of findings.

— ISO/IEC 27043, *Incident investigation principles and processes*

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

— ISO/IEC 27050, *Electronic discovery*

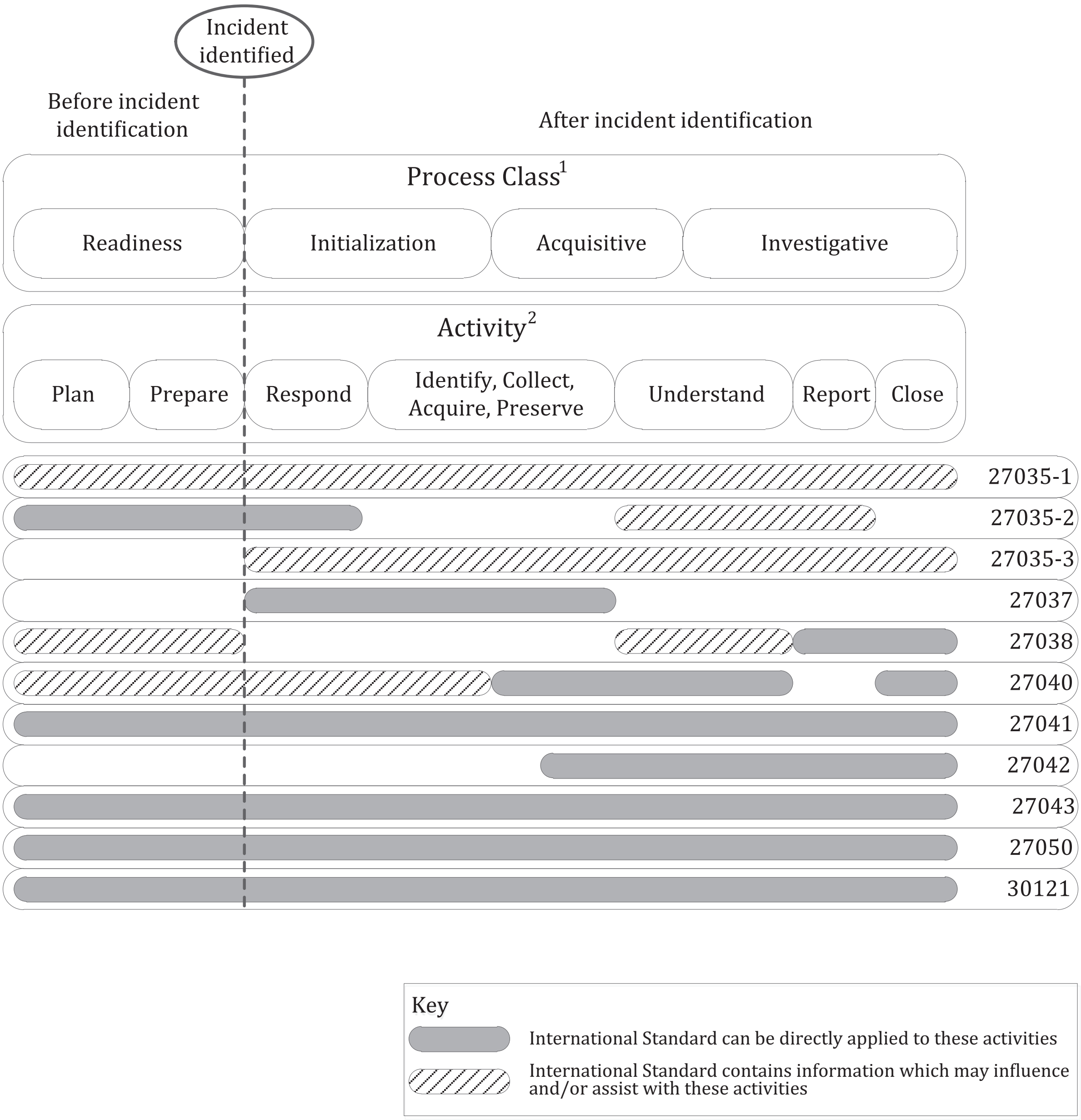
ISO/IEC 27050 addresses activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of Electronically Stored Information (ESI). In addition, it provides guidance on measures, spanning from initial creation of ESI through its final disposition, which an organization can undertake to mitigate risk and expense should electronic discovery become an issue. It is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities. It is important to note that this guidance is not intended to contradict or supersede local jurisdictional laws and regulations.

Electronic discovery often serves as a driver for investigations as well as evidence acquisition and handling activities. In addition, the sensitivity and criticality of the data sometime necessitate protections like storage security to guard against data breaches.

— ISO/IEC 30121, *Governance of digital forensic risk framework*

ISO/IEC 30121 provides a framework for governing bodies of organizations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organization for digital investigations before they occur. ISO/IEC 30121 applies to the development of strategic processes (and decisions) relating to the retention, availability, access and cost effectiveness of digital evidence disclosure. ISO/IEC 30121 is applicable to all types and sizes of organizations. ISO/IEC 30121 is about the prudent strategic preparation for digital investigation of an organization. Forensic readiness assures that an organization has made the appropriate and relevant strategic preparation for accepting potential events of an evidential nature. Actions can occur as the result of inevitable security breaches, fraud, and reputation assertion. In every situation Information Technology (IT) should be strategically deployed to maximise the effectiveness of evidential availability, accessibility and cost efficiency

Figure A.1 shows typical activities surrounding an incident and its investigation. The numbers shown on this diagram (e.g. 27037) indicate the International Standards listed above and the shaded bars show where each is most likely to be directly applicable or has some influence over the investigative process (e.g. by setting policy or creating constraints). It is recommended, however, that all of the International Standards should be consulted prior to, and during, the planning and preparation phases. The process classes shown are defined fully in ISO/IEC 27043 and the activities identified match those discussed in more detail in ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27042 and ISO/IEC 27041.


Incident identified
Before incident identification
After incident identification
Process Class[1]
Readiness
Initialization
Acquisitive
Investigative
Activity[2]
Plan
Prepare
Respond
Identify, Collect, Acquire, Preserve
Understand
Report
Close
27035-1
27035-2
27035-3
27037
27038
27040
27041
27042
27043
27050
30121
Key
International Standard can be directly applied to these activities
International Standard contains information which may influence and/or assist with these activities

1. Process classes are defined in ISO/IEC 27043
2. Detail of activities is given in ISO/IEC 27035-2, ISO/IEC 27037, and ISO/IEC 27042

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

Annex B
(informative)

Examples of information security incidents and their causes

B.1 Attacks

B.1.1 Denial of Service

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

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

— pinging network broadcast addresses in order to fill up network bandwidth with response traffic;

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

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

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

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

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

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

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

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

— system malfunctions or overload,

— uncontrolled system changes, and

— malfunctions of software or hardware.

B.1.2 Unauthorized access

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

- attempts to retrieve password files,
- buffer overflow attacks to attempt to gain privileged (e.g. system administrator) access to a target,
- exploitation of protocol vulnerabilities to hijack or misdirect legitimate network connections, and
- attempts to elevate privileges to resources or information beyond what a user or administrator already legitimately possesses.

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

- breaches of physical security arrangements resulting in unauthorized access to information, and
- poorly and/or mis-configured operating systems due to uncontrolled system changes, or malfunctions of software or hardware.

B.1.3 Malware

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

B.1.4 Abuse

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

- downloading and installing hacking tools,
- using corporate e-mail for spam or promotion of personal business,
- using corporate resources to set up an unauthorized web site, and
- using peer-to peer activities to acquire or distribute pirated files (music, video, software).

B.2 Information gathering

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

- existence of a target, and to understand the network topology surrounding it, and with whom the target routinely communicates, and
- potential vulnerabilities in the target or its immediate network environment that could be exploited.

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

- dumping Domain Name System (DNS) records for the target's Internet domain (DNS zone transfer);

- pinging network addresses to find systems that are “alive”;
- probing the system to identify (e.g. fingerprint) the host operating system;
- scanning the available network ports on a system to identify network services (e.g. e-mail, File Transfer Protocol (FTP), web, etc.) and the software versions of those services;
- scanning for one or more known vulnerable services across a network address range (horizontal scanning).

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

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

- direct or indirect disclosure or modification information,
- theft of intellectual property stored electronically,
- breaches of accountability, e.g. in account logging, and
- misuse of information systems (e.g. contrary to law or organization policy).

Information gathering incidents could be caused, for example, by

- breaches of physical security arrangements resulting in unauthorized access to information, and theft of data storage equipment that contains important data, for example encryption keys,
- poorly and/or misconfigured operating systems due to uncontrolled system changes, or malfunctions of software or hardware, resulting in internal or external personnel gaining access to information for which they have no authority, and
- social engineering, which is an act of manipulating people into performing actions or divulging confidential information, e.g. phishing.

Annex C
(informative)

Cross reference table of ISO/IEC 27001 vs ISO/IEC 27035

ISO/IEC 27001:2013	ISO/IEC 27035
A.16 Information security incident management	**ISO/IEC 27035-1:** **4 Overview** (for the overview of information security incident management)
A.16.1 Management of information security incidents and improvements Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	**ISO/IEC 27035-1**: **5 Phases** (for the phases of information security incident management) **Annex B (informative) Examples of information security incidents and their causes** **ISO/IEC 27035-2**: **Annex A (informative) Legal and regulatory aspects** **ISO/IEC TS 27035-3**: **5 Incident response operations** **Annex A (informative) Example of the incident criteria based on computer security events and incidents** **Annex B (informative) Example information security event, incident and vulnerability reports and forms** **Annex C (informative) Example approaches to the categorization and classification of information security events and incidents**

ISO/IEC 27001:2013	ISO/IEC 27035
A.16.1.1 Responsibilities and procedures Control: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	**ISO/IEC 27035-1:** 5.2 **Plan and Prepare** 5.4 **Assessment and Decision** a), b) **ISO/IEC 27035-2:** **4 Information security incident management policy** **5 Updating of information security policies** **6 Creating information security incident management plan** **7 Establishing an Incident Response Team (IRT)** **8 Establishing relationships with other organizations** **9 Defining technical and other support** **10 Creating information security incident awareness and training** **ISO/IEC TS 27035-3:** **5.1 Incidents** **5.2 Incident response processes**
A.16.1.2 Reporting information security events Control: Information security events shall be reported through appropriate management channels as quickly as possible.	**ISO/IEC 27035-1:** 5.3 **Detection and Reporting** **ISO/IEC TS 27035-3:** **5.3 Detection and Reporting**
A.16.1.3 Reporting information security weaknesses Control: Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	**ISO/IEC 27035-1:** 5.3 **Detection and Reporting**
A.16.1.4 Assessment of and decision on information security events Control: Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	**ISO/IEC 27035-1:** 5.4 **Assessment and Decision** **ISO/IEC TS 27035-3:** **5.4 Assessment and Decision**
A.16.1.5 Response to information security incidents Control: Information security incidents shall be responded to in accordance with the documented procedures.	**ISO/IEC 27035-1:** **5.5 Responses** **ISO/IEC TS 27035-3:** **5.5 Responses** **5.6 Post Incident Activity** **6 General known incident response**
A.16.1.6 Learning from information security incidents Control: Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	**ISO/IEC 27035-1:** **5.6 Lessons Learnt** **ISO/IEC 27035-2:** **12 Lessons Learnt**

ISO/IEC 27001:2013	ISO/IEC 27035
A.16.1.7 Collection of evidence Control: The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	**ISO/IEC 27035-1:** **5.3 Detection and Reporting** d), g) **5.4 Assessment and Decision** d), g) **5.5 Responses** d), i), l) **ISO/IEC TS 27035-3:** **5.3 Detection and Reporting** **5.4 Assessment and Decision** **5.5 Responses**

Bibliography

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

[2] ISO/PAS 22399,[3]*Societal security — Guidelines for incident preparedness and operational continuity management*

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

[4] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[5] ISO/IEC 27003,[4]*Information technology — Security techniques — Information security management system implementation guidance*

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

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

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

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

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

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

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

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

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

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

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

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

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

[19] APCERT. Member Teams, http://www.apcert.org/about/structure/members.html

[3] Withdrawn.

[4] To be published.

[5] To be published.

[20] ENISA. Inventory of CERT activities in Europe (v.2.10), June 2013, http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe/at_download/fullReport

[21] FIRST. Alphabetical list of FIRST Members, http://www.first.org/members/teams

[22] NIST SP 800-61, *Computer Security Incident Handling Guide* (2012*)* http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

[23] IETF RFC 2196, *Site Security Handbook*, http://www.ietf.org/rfc/rfc2196.txt?number=2196

[24] IETF RFC 2350, *Expectations for Computer Security Incident Response*, http://www.ietf.org/rfc/rfc2350.txt?number=2350

[25] IETF RFC 5070, *The Incident Object Description Exchange Format (IODEF)*

[26] IETF RFC 3227, *Guidelines for evidence collection and archiving*

[27] CESG GOVCERTUK. *Incident Response Guidelines (* 2008*)*, https://www.cesg.gov.uk/

[28] Software Engineering Institute at Carnegie Mellon. CERT Coordination Center", *Incident Management Capability Metrics Version 0.1 (* 2007*)*, http://www.cert.org/archive/pdf/07tr008.pdf

[29] Software Engineering Institute at Carnegie Mellon. CERT Coordination Center", *Incident Management Mission Diagnostic Method Version 1.0*, http://www.cert.org/archive/pdf/08tr007.pdf

[30] Software Engineering Institute at Carnegie Mellon. CERT Coordination Center", Defining Incident Management Processes for CSIRTs: A Work in Progress, http://www.cert.org/archive/pdf/04tr015.pdf

[31] Software Engineering Institute at Carnegie Mellon. CERT Coordination Center", Handbook for Computer Security Incident Response Teams (CSIRTs), http://www.cert.org/archive/pdf/csirt-handbook.pdf

[32] Software Engineering Institute at Carnegie Mellon. CERT Coordination Center", State of the Practice of Computer Security Incident Response Teams, http://www.cert.org/archive/pdf/03tr001.pdf

[33] Software Engineering Institute at Carnegie Mellon. CERT Coordination Center", CSIRT Services, http://www.cert.org/csirts/services.html

[34] Software Engineering Institute at Carnegie Mellon. CERT Coordination Center", Action List for Developing a Computer Security Incident Response Team (CSIRT), http://www.cert.org/csirts/action_list.html

[35] Software Engineering Institute at Carnegie Mellon. CERT Coordination Center", *Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?* http://www.cert.org/csirts/csirt-staffing.html

[36] Software Engineering Institute at Carnegie Mellon "CERT Coordination Center", *Steps for Creating National CSIRTs*, http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

[37] SANS Institute, *An approach to the ultimate in-depth security event management framework (2008)*

[38] SANS Institute. Mining gold, A primer on incident handling and response *(* 2008*)*

[39] SANS Institute. Incident Handling for SMEs (Small to Medium Enterprises) *(* 2008*)*

[40] SANS Institute. Breach Notification in Incident Handling *(* 2008*)*

[41] SANS Institute. Baselines and Incident Handling *(* 2008*)*

[42] SANS Institute. Documentation is to Incident Response as an Air Tank is to Scuba Diving *(* 2007*)*

[43] SANS Institute. Creating and Managing an Incident Response Team for a Large Company *(* 2007*)*

[44] SANS Institute. An Incident Handling Process for Small and Medium Businesses *(* 2007*)*

[45] SANS Institute. Incident Management 101 Preparation & Initial Response (aka Identification) *(* 2005*)*

[46] SANS Institute. Building an Incident Response Program To Suit Your Business *(* 2003*)*

[47] ISACA, *COBIT 4.1 (Section DS5.11)*, www.isaca.org/cobit

[48] ENISA. *A step-by-step approach on how to set up a CSIRT*, http://www.enisa.europa.eu/act/cert/support/guide

[49] ENISA. *CERT cooperation and its further facilitation by relevant stakeholders*, http://www.enisa.europa.eu/act/cert/background/coop

[50] ENISA. *A basic collection of good practices for running a CSIRT*, http://www.enisa.europa.eu/act/cert/support/guide2

[51] TERENA's *Incident Object Description and Exchange Format Requirements (IODEF) (produced by IETF), RFC 3067*

[52] CVSS, *A complete Guide to the Common Vulnerability Scoring System (Version 2.0), FIRST, 20 June* 2007, http://www.first.org/cvss/cvss-guide.html

[53] SWIF, *Structured Warning Information Format (Version 2.3), ITsafe, 9 May 2008*

[54] ITIL. *ITIL framework document*, http://www.itil-officialsite.com/home/home.asp

[55] Ten Strategies of a World-Class Cybersecurity Operations Center, https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

[56] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

ICS 35.040

Price based on 25 pages

REPORT OF VOTING ON ISO/IEC DIS 27035-1	
Closing date of voting **2015-10-29**	**ISO/IEC JTC 1/SC 27**
Secretariat **DIN**	

A report shall be returned to ISO/CS no later than 3 months after the closing date of voting on the DIS.

1 **Result of the voting**

The above-mentioned document was circulated to member bodies with a request that the ISO Central Secretariat be informed whether or not member bodies were in favour of registration of the DIS for publication.
The vote closed on the date indicated above. The replies listed in annex A have been received.

2 **Comments received**

3 **Observations of the secretariat**

See annex B (separetely circulated as N15525)

4 **Decision of the Chairman**

Where the approval criteria are met:

□ A revised text is to be submitted to ISO/CS for publication *(No FDIS)*

☒ A revised text is to be submitted to ISO/CS for the approval procedure *(Optional FDIS implementation)*

Where the approval criteria are not met:

□ A revised text is to be submitted to ISO/CS for a further enquiry (DIS) vote

□ The project is to revert to the Committee Stage (a new committee draft will be developed)

□ The enquiry draft and comments will be discussed at the next meeting

Remarks (e.g. observations on how comments were reviewed, date by which a decision is to be taken, date when a text is expected)

The DIS document was circulated as SC 27 N15421. The summary of voting is presented in N15525. The dispositions of NB comments (refer to SoV SC 27 N15525) are shown in N15795. The text for a 2-month FDIS balloting is presented in N15796. It was submitted to ITTF for a FDIS ballot processing on 2016-01-07.

The US NB negative vote was satisfactorily resolved and changed to approval.

Enclosures

☒ **Annex A** *(DIS results from ISO electronic balloting portal)*

☒ **Annex B** *(comments received with observations of the secretariat separately circulated as N15795)*

Signature of the Secretary	Signature of the Chairman
Passia, Krystyna Mrs	Fumy Walter Mr
Date **2016-01-07**	Date **2016-01-07**

Ballot Information

Reference	ISO/IEC DIS 27035-1	**Committee**	ISO/IEC JTC 1/SC 27
Edition number	1		
English title	Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management		
French title	Technologies de l'information -- Techniques de sécurité -- Gestion des incidents de sécurité de l'information -- Partie 1:		
Start date	2015-07-27	**End date**	2015-10-27
Opened on	2015-07-27 00:03:46	**Closed on**	2015-10-29 00:00:42
Status	Closed		
Voting stage	Enquiry	**Version number**	1
Note			

Result of voting

P-Members voting: 18 in favour out of 19 = 95 % (requirement >= 66.66%)

(P-Members having abstained are not counted in this vote.)

Member bodies voting: 1 negative votes out of 27 = 4 % (requirement <= 25%)

Approved

Votes by members

Country	Member	Status	Approval	Disapproval	Abstention
Argentina	IRAM	O-Member	X *		
Australia	SA	P-Member	X		
Austria	ASI	P-Member			X
Belgium	NBN	P-Member	X		
Canada	SCC	P-Member	X		
Chile	INN	O-Member			X
China	SAC	P-Member	X *		
Costa Rica	INTECO	P-Member			X
Côte d'Ivoire	CODINORM	P-Member			X
Cyprus	CYS	O-Member	X		
Czech Republic	UNMZ	P-Member	X		
Denmark	DS	P-Member	X		

Ethiopia	**ESA**	**O-Member**	X		
Finland	**SFS**	**P-Member**			X
France	**AFNOR**	**P-Member**	X		
Germany	**DIN**	**P-Member**			X
India	**BIS**	**P-Member**	X		
Ireland	**NSAI**	**P-Member**	X		
Italy	**UNI**	**P-Member**			X
Japan	**JISC**	**P-Member**	X *		
Kazakhstan	**KAZMEMST**	**P-Member**	X		
Korea, Republic of	**KATS**	**P-Member**	X		
Lebanon	**LIBNOR**	**P-Member**	X		
Malaysia	**DSM**	**P-Member**			X
Malta	**MCCAA**	**P-Member**			X
Mexico	**DGN**	**O-Member**	X		
Netherlands	**NEN**	**P-Member**			X
Nigeria	**SON**	**P-Member**			
Norway	**SN**	**P-Member**	X		
Peru	**INACAL**	**P-Member**	X		
Poland	**PKN**	**O-Member**	X		
Russian Federation	**GOST R**	**P-Member**			X
Rwanda	**RSB**	**O-Member**	X		
Singapore	**SPRING SG**	**P-Member**	X		
South Africa	**SABS**	**P-Member**			X
Spain	**AENOR**	**P-Member**			X
Sweden	**SIS**	**P-Member**	X		
Switzerland	**SNV**	**P-Member**			X
Thailand	**TISI**	**O-Member**	X		
Ukraine	**DTR**	**O-Member**	X		
United Arab Emirates	**ESMA**	**P-Member**	X		
United Kingdom	**BSI**	**P-Member**			X
United States	**ANSI**	**Secretariat**		X *	
P-Member TOTALS Total of P-Members voting: 19			18	1	14
TOTALS			26	1	15
(*) A comment file was submitted with this vote					

Comments from Voters			
Argentina	**IRAM**	**O-Member**	
China	**SAC**	**P-Member**	
Japan	**JISC**	**P-Member**	
United States	**ANSI**	**Secretariat**	

Title:	Information security incident management – Part 1: Principles of incident management				**Date**: 2015-10-30	**Document:** SC 27 N15795	**Project:** ISO/IEC 27035-1
Type:	Disposition of comments		**Stage:**	DIS			
References:	*Draft:*	SC 27 N15421	*SoC:*	SC 27 N15525			

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
JP-1				Ge	The term “this international standard” is used throughout this document, which will not refer to 27035-1 only but all three parts. Because part 3 has moved to TS not IS, the validity of the term should be checked.	Discuss the comment at the meeting.	Accepted in principle “ISO/IEC 27035” Directives part 2 6.6.7.2
US-1		Forward, throughout		ge	With the change in how Part 3 is going to be developed, should the foreword be updated to remove reference to it as a part of the ISO standard and a reference instead be added as a technical specification (TS)?	Remove “Part 3: Guidelines for incident response operations.” Add Additional information to supplement ISO/IEC 27035 can be found in the technical specification “Guidelines for incident response operations” Make similar consistent changes throughout the document whenever part 3 is mentioned, such as “about this standard” or “normative references”	Accepted in principle Also see CN-1, CN-3, JP-2 *Editor Note: One solution is to add a note ”Under development” to “ISO/IEC TS 27035-3”.* *“*ISO/IEC TS 27035-3, *Guidelines for incident response operations*,”
CN-1		0.1	Para2 Item3	ed	ISO/IEC 27035-3 project has been changed to TS.	Change ISO/IEC 27035-3, To ISO/IEC TS 27035-3,	Accepted
CN-2		0.2	Para-1	ed	Swap Annex A and Annex B to follow the editing rule for Annex specified in ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, 5.2.6 Annex, which says “Annexes shall appear in the order in which they are cited in the text.”	Change Annex B. To Annex A.	Accepted
CN-3		2	Para-1	ed	ISO/IEC 27035-3 project has been changed to TS.	Change ISO/IEC 27035-3, To ISO/IEC TS 27035-3,	Accepted
JP-2		2		Ed	ISO/IEC 27035-3 has been moved to TS not IS. Change the product type accordingly.	Change “ISO/IEC 27035-3” to “ISO/IEC TS 27035-3”	Accepted Also see CN-3

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
CN-4		3.1	Para2	ed	ISO/IEC 27042 has been published.	Change ISO/IEC 27042[1], To ISO/IEC 27042:2015,	Not accepted Reference to undated version indicates most recently published version Not necessary to cite dated version, definition in 3.1 is modified from source
JP-3		3.1	Footnote 1	Ed	ISO/IEC 27042:2015 is published so the current footnote 1 “To be published.” Is irrelvent.	Remove footnote 1.	Accepted Also see CN-4
JP-4		3.1		Ed	Grammatical error	Change The words “an incident” was … To The words “an incident” were …	Accepted in principle Changed to: The phrase “an incident” was replaced by “an information security incident”.
CN-5		3.7	Para2	ed	The source reference should be dated.	Change SOURCE: ISO/IEC 27039, 2.24, To SOURCE: ISO/IEC 27039:2015, 2.24,	Not accepted For undated references, the latest edition of the referenced document (including any amendments) applies.
US-2		3.7 incident response	Paragraph	Te	Incident response normally involves trying to mitigate or resolve the incident. The current definition does not clearly address those actions. Mitigation is different from protection and restoration of normal operational conditions.	Change “action taken to protect and restore the normal operational conditions…” To “actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.” Remove or modify SOURCE: if needed.	Accepted in principle Removed reference to 27039, which is about IDPS

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
US-3		3.8 Point of Contact	Paragraph	Te	During an incident there may be many different POCs depending on the organizations involved. This definition as written seems to imply there is only one. Perhaps it needs to address there may be more than one.	Change “defined organizational function or role serving as the coordinator or focal point of information concerning incident management activities” To “defined organizational function or role serving as the coordinator or focal point of information concerning particular incident management activities” NOTE: There may be more than one PoC involved during an incident. For example, a PoC can be a lead analyst for the response actions, there can be a PoC at a victim site to coordinate mitigations and information, and there could be a PoC in media relations, if the incident has become public knowledge.	Not accepted Existing definition already addresses
US-4		4.1 Basic concepts and principles	Paragraph 1 and 2	Te	Information security events are normally assessed against a criteria or threshold set by an organization once detected. If they met the threshold – then an information security incident is declared. The sentence “An information security incident is one or multiple related and identified information security events that can harm an organization's assets or compromise its operations.” can cause some confusion, in interpretation and can miss this fine point.	Replace first to paragraphs of 4.1 with: “An information security event is an occurrence indicating activity that could potentially harm an organization’s assets or compromise its operations. When information security events are identified they are measured against criteria set by an organization to determine if an information security incident should be declared (or: if the events should be classified as an information security incident). Such a declaration involves invoking organizational incident handling processes to resolve or mitigate the information security incident. The occurrence of an information security event does not necessarily mean that an attack has been successful or that there are any implications on confidentiality, integrity or availability, i.e., not all information security events are classified as information security incidents.”	Accepted in principle “An information security incident is one or multiple related and identified information security events that meet established criteria and can harm an organization's assets or compromise its operations.”
CN-6		4.1	Para4	ed	Swap Annex A and Annex B to follow the editing rule for Annex specified in ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, 5.2.6 Annex, which says “Annexes shall appear in the order in which they are cited in the text.”	Change Annex A. To Annex B.	Accepted

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
CN-7		4.2	Para2 e)	ed	Use plural.	Change some other team To some other teams	Accepted
CN-8		4.2	Figure 2	ed	Correct grammar error.	Change Shares information with To Share information with	Accepted
US-5		4.2 Objectives of Incident Managemen t	Last paragraph	ge	The term ISMS is used in the paragraph but not defined. For better comprehension it should be explained to those who are not familiar with it.	In the second line of the paragraph change "ISMS" To information security management system (ISMS)	Accepted
CN-9		4.3	Para1 e) Subpara1 Line4	ed	Swap Annex A and Annex B to follow the editing rule for Annex specified in ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, 5.2.6 Annex, which says "Annexes shall appear in the order in which they are cited in the text."	Change Annex B. To Annex A.	Accepted
US-6		4.4 Adaptability	Bullet a)	te	Any incident management capability should be looked in light of risk management. A key first step is to identify the types of critical assets and key business processes and data that must be protected. This sentiment should be alluded to with clearer language.	Change bullet a) Size, structure, and business nature of an organization To Size, structure, and business nature of an organization including key critical assets, processes, and data that must be protected	Accepted in principle "a) size, structure and business nature of an organization including key critical assets, processes, and data that should be protected,"
US-7		4.4 Adaptability	Bullet c)	te	Any incident management capability should be looked in light of risk management. A key first step is to identify the types of critical assets and key business processes and data that must be protected. This sentiment should be alluded to with clearer language.	Change bullet c) Potential loss through unprevented incidents, and To Potential risk due to unprevented incidents, and	Accepted

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
US-8		5.1 overview	Box of bullets for Plan and Prepare	te	Building on the importance of understanding the critical assets to protect, identifying what those are should be part of the plan and prepare – if not already done by the organization. If it is done, then it should be used to help develop requirements. Risk assessment information should also be incorporated. Note if any of these additions are made they will also need to be addressed in 5.2 Plan and Prepare	Add bullet at beginning of Plan and Prepare or add new paragraph to address these topics before Plan and prepare boxes for - Risk assessment, to include identification of assets, processes, data, and threats	Not accepted Risk assessment is a part of risk management which should be done before and be being done throughout information security incident management. Asset identification part of risk management is emphasized in other accepted comments.
CN-10		5.1	Para-2 Item3	ed	ISO/IEC 27035-3 project has been changed to TS.	Change ISO/IEC 27035-3, To ISO/IEC TS 27035-3,	Accepted
US-14		5.2	c)	te	Incorporate or develop organizational and IRT communications and information disclosure plans as a critical part of the overall incident management plan. See US-13 and corresponding comment US-24 on 27035-2.	Change 5.2 c) to: Define and document a detailed information security incident management plan, including topics covering communications and information disclosure.	Accepted
AR-1		5.2	f)	Ed	"the IRT., Develop" should be "the IRT. Develop".	the IRT. Develop	Accepted
CN-11		5.3	Para3 f) Line4	ed	Swap Annex A and Annex B to follow the editing rule for Annex specified in ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, 5.2.6 Annex, which says "Annexes shall appear in the order in which they are cited in the text."	Change Annex B. To Annex A.	Accepted
US-10		5.3 Detection and Reporting And also 5.5 Responses	Last paragraph in each section	Ge	Update reference to part 3 as a TS, see US-1.	Re-word Part 3 of this International Standard describes in detail each of the activities listed above. To instead point to the appropriate technical specification, as Part 3 is being removed.	Accepted in principle See US-1 "Part 3 of ISO/IEC 27035 describes…"
US-9		5.5 Responses			Analysis is a key part of the incident handling process. Although "investigation" is called out in this model/standard. It does not show as much focus as is warranted on the types of analysis that might occur. Investigation is a type/subset of analysis, but is	In the 5.5 Response section add at end of bullet d) Investigation can include many different kinds of analysis to provide a more in depth understanding of what happened (i.e., how the intruder or attacker may have gotten into to the organizational systems; what data or assets or operations have been affected and how they have been affected,	Accepted in principle Added to 5.5 d) "Investigation can include different kinds of analyses to provide a more in-depth understanding of incidents."

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
					used here as a synonym?	how severe the malicious activity was, if the attack vector or modus operandi is known or new, if any mitigations already exist. Analysis activities can also be iterative, as more information is uncovered and interpreted, more analysis may need to be performed. Analysis performed can include but is not limited to - Incident Analysis – identifying the timeframe, scope, success of the malicious activity; along with determining the type and class of incident. - Technical Vulnerability Analysis – identifying vulnerabilities in software or hardware and how they were able to be exploited by attackers - Malware and Artefact Analysis – understanding the functionality and use of malware and other artefacts used to enact attacks and other malicious activity - Digital Media Analysis - analysis of relevant data from systems, networks, digital storage, and removable media in order to better understand how to prevent, detect, and/or mitigate similar or related incidents. - Business Impact Analysis – determining how the malicious activity has impacted organizational or constituent operations and what type of outcomes are expected such as downtime of services, decrease in productivity, loss of funds, loss of life, or loss of sensitive or personally identifying data.	Too much detail for a bullet point in part 1, proposed text forwarded to editors of part 3.
CN-12		5.5	Para3 i)	ed	Swap Annex A and Annex B to follow the editing rule for Annex specified in ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, 5.2.6 Annex, which says “Annexes shall appear in the order in which they are cited in the text.”	Change Annex B. To Annex A.	Accepted

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
US-13		5.5	Bullet k)	te	Any type of communication should occur in accordance with organizational and/or IRT communications plans and in alignment with any information disclosure policies. US-13: Information sharing/disclosure should be in accordance with plan/policy. US-14: Develop plan/policy first.	Change the first sentence of bullet k) from Communicate the existence of the information security incident and share any relevant details (e.g.,threat, attack, and vulnerability information) with other internal and external individuals or organizations. to Communicate the existence of the information security incident and share any relevant details (e.g. threat, attack, and vulnerability information) with other internal and external individuals or organizations, in accordance with organizational and IRT communication plans and information disclosure policies.	Accepted
US-11		5.5 responses	Bullet L.1 and L.2	te	The first two bullets related to Post Incident Activity do not have enough context to clearly identify their meaning. 1) Investigation of the stored information; Investigation of the information how? What is being looked for that is not already known? 2) Investigation of other relevant sources such as involved personnel; What personnel should be investigated, and what is the outcome? Why are they being investigated?	Add additional information to the bullets to convey context and clarify actions. I am not sure what is being said, so I'm not sure how to change it. Remove if there is no known meaning.	Accepted in principle End of 5.5 refers to part 3 for further information Changed "stored information" to "…information pertaining to the incident;"
CN-13		5.5	Para3 l) 4)	ed	Correct wrong numbering.	Change 4) Once the incident has been resolved, To m) Once the incident has been resolved,	Accepted

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
US-12		Section 5.6 Lessons Learnt	Bullet g)	Ed	There are missing words from the bullet sentence that makes it difficult to read or understand.	Change: g) Perform a comprehensive evaluation IRT performance and effectiveness on a periodic basis. To g) Perform a comprehensive evaluation of IRT performance and effectiveness on a periodic basis.	Accepted
CN-14		Annex A	Title	ed	Swap Annex A and Annex B to follow the editing rule for Annex specified in ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, 5.2.6 Annex, which says "Annexes shall appear in the order in which they are cited in the text."	Change Annex A. To Annex B.	Accepted
CN-15		Annex B	Title	ed	Swap Annex A and Annex B to follow the editing rule for Annex specified in ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, 5.2.6 Annex, which says "Annexes shall appear in the order in which they are cited in the text."	Change Annex B To Annex A	Accepted
CN-16		Annex B	Para1 Item2 Subpara1	ed	ISO/IEC 27038 has been published.	Change *[Status: at the time of writing, this international standard was being prepared for publication]* To *[Status: This international standard was published in 2014]*	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text
JP-6		Annex B		Ed	ISO/IEC 27038 is published as ISO/IEC 27038:2014 so the corresponding text should be updated as proposed.	Remove the following sentence: *[Status: at the time of writing, this international standard was being prepared for publication]* Also, editor is recommended to check the current text to make sure that the published 27038:2014 and the current text is consistent.	Accepted in principle Also see CN-16 Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
JP-5		Annex B		Ed	The use of the term 'must' should be avoided.	Change 'must' to 'should'.	Accepted SD3 is defunct, modifying Annex B as needed *Editor Note: The text is a copy from the published ISO/IEC 27038:2014.*
CN-17		Annex B	Para1 Item3 Subpara1	ed	ISO/IEC 27040 has been published.	Change *[Status: at the time of writing, this international standard was in development]* To *[Status: This international standard was published in 2015]*	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text
JP-7		Annex B		Ed	Same as the above comment, ISO/IEC 27040 is published as ISO/IEC 27040:2015 so the corresponding text should be updated as proposed.	Remove the following sentence: *[Status: at the time of writing, this international standard was in development]* Also, editor is recommended to check the current text to make sure that the published 27040:2015 and the current text is consistent.	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text
CN-18		Annex B	Para1 Item4 Subpara1	ed	ISO/IEC 27041 has been published.	Change *[Status: at the time of writing, this international standard was in development]* To *[Status: This international standard was published in 2015]*	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text
JP-8		Annex B		Ed	Same as the above comment, ISO/IEC 27041 is published as ISO/IEC 27041:2015 so the corresponding text should be updated as proposed.	Remove the following sentence: *[Status: at the time of writing, this international standard was in development]* Also, editor is recommended to check the current text to make sure that the published 27041:2015 and the current text is consistent.	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
CN-19		Annex B	Para1 Item5 Subpara1	ed	ISO/IEC 27042 has been published.	Change *[Status: at the time of writing, this international standard was in development]* To *[Status: This international standard was published in 2015]*	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text
JP-9		Annex B		Ed	Same as the above comment, ISO/IEC 27042 is published as ISO/IEC 27042:2015 so the corresponding text should be updated as proposed.	Remove the following sentence: *[Status: at the time of writing, this international standard was in development]* Also, editor is recommended to check the current text to make sure that the published 27042:2015 and the current text is consistent.	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text
CN-20		Annex B	Para1 Item6 Subpara1	ed	ISO/IEC 27043 has been published.	Change *[Status: at the time of writing, this international standard was in development]* To *[Status: This international standard was published in 2015]*	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text
JP-10		Annex B		Ed	Same as the above comment, ISO/IEC 27043 is published as ISO/IEC 27043:2015 so the corresponding text should be updated as proposed.	Remove the following sentence: *[Status: at the time of writing, this international standard was in development]* Also, editor is recommended to check the current text to make sure that the published 27043:2015 and the current text is consistent.	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text
AR-2		Annex B	ISO/IEC 27044 Guidelines for security information and event management (SIEM)	Ed	Unnecessary uppercases “Management Processes/Systems” should be “Management processes/systems”. Even SIEM could be in lowercase.	Management processes/systems	Overtaken by events 27044 has been cancelled and references removed from 27035 Also see CN-21

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
CN-21		Annex B	Para1 Item7 Subpara1	ed	ISO/IEC 27044 project has been canceled.	Delete —▪ISO/IEC 27044 Guidelines for security information and event management (SIEM) *[Status: at the time of writing, this international standard was in development]* This provides guidelines to organizations in preparing to deploy Security Information & Event Management Processes/Systems. In particular, it addresses the selection, deployment and operations of SIEM. It intends specifically to offer assistance in satisfying requirements of ISO/IEC 27001:2005: regarding the implementation of procedures and other controls capable of enabling prompt detection and response to security incidents, to execute monitoring and review procedures to properly identify attempted and successful security breaches and incidents.	Accepted Need to update figure A.1
JP-11		Annex B		Ed	ISO/IEC 27044 is dropped at the previous meeting at Kuchin thus the entire bullet about ISO/IEC 27044 should be removed from the text	Remove the following text: ISO/IEC 27044 Guidelines for security information and event management (SIEM) [Status: at the time of writing, this international standard was in development] This provides guidelines to organizations in preparing to deploy Security Information & Event Management Processes/Systems. In particular, it addresses the selection, deployment and operations of SIEM. It intends specifically to offer assistance in satisfying requirements of ISO/IEC 27001:2005: regarding the implementation of procedures and other controls capable of enabling prompt detection and response to security incidents, to execute monitoring and review procedures to properly identify attempted and successful security breaches and incidents.	Accepted Also see CN-21 Update figure A.1
CN-22		Annex B	Para1 Item9 Subpara1	ed	ISO/IEC 30121 has been published.	Change *[Status: at the time of writing, this international standard was being prepared for publication]* To *[Status: This international standard was published in 2015]*	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
JP-12		Annex B		Ed	ISO/IEC 30121 is published as ISO/IEC 30121:2015 so the corresponding text should be updated as proposed.	Remove the following sentence: *[Status: at the time of writing, this international standard was being prepared for publication]* Also, editor is recommended to check the current text to make sure that the published 30121:2015 and the current text is consistent.	Accepted in principle Undated references Update all of Annex B (content from SD3) to reflect published and cancelled standards Update or remove figure A.1 and associated text
CN-23		Annex B	Figure A.1	ed	ISO/IEC 27044 project has been canceled.	Delete 27044	Accepted Need figure source or create new figure
JP-13		Annex B	Figure A.1	Ed	27044 does not exist (see JP-7) thus it should be removed from the figure.	Remove 27044 from the figure.	Accepted Also see CN-23
JP-14		Annex B	Figure A.1	Ed	The numbering of the figure is wrong. Also change colon to dash.	Change Figure A.1 : Applicability of standards to investigation process classes and activities to Figure B.1 — Applicability of standards to investigation process classes and activities	Overtaken by events See CN-15.
JP-15		Annex C		ed	The headings of the table are "… Clause". However, the listed items contain not only clause but also subclause.	Change "… Clause" to "… clause/subclause"	Accepted in principle Delete "clause" from heading rows
CN-24		Annex C	Table Row3 Col2 Part 1 Annex A	ed	Swap Annex A and Annex B to follow the editing rule for Annex specified in ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, 5.2.6 Annex, which says "Annexes shall appear in the order in which they are cited in the text."	Change Annex A. To Annex B.	Accepted
CN-25		Annex C	Table Row4 Col2 Part 2 8&9	ed	Keep consistent with Part 2.	Change 8 Defining technical and other support 9 Creating information security incident awareness and training To 8 Establishing relationships with other organizations 9 Defining technical and other support 10 Creating information security incident awareness and training	Accepted

MB	Line number	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment	Comments	Proposed change	Observations of the secretariat
CN-26		Annex C	Table Row4 Col2 Part 3 5.1	ed	Keep consistent with Part 3.	Change 5.1 Incident criteria To 5.1 Incidents	Accepted
CN-27		Annex C	Table Row9 Col2 Part 2 11	ed	Correct wrong reference number and add lost "s".	Change 11 Lesson Learnt To 12 Lessons Learnt	Accepted
CN-28		Annex C	Table Row10 Col2 Part 1 5.3	ed	Add missing reference number.	Change 5.3 Detection and Reporting d) To 5.3 Detection and Reporting d), g)	Accepted
JP-16		Bibliography	[7]	Ed	27005 is included in the a normative references thus it should be removed from the bibliography.	Remove [7]	Accepted
CN-29		Bibliography	[15]	ed	ISO/IEC 27041 has been published.	Change ISO/IEC 27041[2], To ISO/IEC 27041,	Accepted
CN-30		Bibliography	[16]	ed	ISO/IEC 27042 has been published.	Change ISO/IEC 27042[3], To ISO/IEC 27042,	Accepted
CN-31		Bibliography	[17]	ed	ISO/IEC 27043 has been published.	Change ISO/IEC 27043[4], To ISO/IEC 27043,	Accepted
JP-18		Bibliography	Footnote2, 3 and 5	Ed	The corresponding standards have been published thus the footnotes should be removed	Remove footnote 2,3 and 5	Accepted Also see CN-29, CN-30, CN-31
CN-32		Bibliography	[18]	ed	ISO/IEC 27044 project has been canceled.	Delete [18] ISO/IEC 27044[5], Information technology — Security techniques — Security Information and Event Management (SIEM)	Accepted
JP-17		Bibliography	[18]	Ed	Same as above reason, item [18] should be removed from the text	Remove [18]	Accepted Also see CN-32