BS ISO/IEC 27035:2011

BSI Standards Publication

Information technology — Security techniques — Information security incident management

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 27035:2011

National foreword

This British Standard is the UK implementation of ISO/IEC 27035:2011. It supersedes PD ISO/IEC TR18044:2004 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2011

ISBN 978 0 580 63587 8

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2011.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27035:2011

INTERNATIONAL STANDARD

ISO/IEC 27035

First edition
2011-09-01

Information technology — Security techniques — Information security incident management

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

Reference number
ISO/IEC 27035:2011(E)

Documents
Document Sharing Hub

© ISO/IEC 2011

Full document details: BS ISO/IEC 27035:2011

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27035:2011

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Overview 2
4.1 Basic concepts 2
4.2 Objectives 3
4.3 Benefits of a structured approach 4
4.4 Adaptability 5
4.5 Phases 6
4.6 Examples of information security incidents 7

5 Plan and prepare phase 8
5.1 Overview of key activities 8
5.2 Information security incident management policy 10
5.3 Information security incident management integration in other policies 12
5.4 Information security incident management scheme 13
5.5 Establishment of the ISIRT 18
5.6 Technical and other support (including operational support) 19
5.7 Awareness and training 20
5.8 Scheme testing 22

6 Detection and reporting phase 22
6.1 Overview of key activities 22
6.2 Event detection 25
6.3 Event reporting 25

7 Assessment and decision phase 26
7.1 Overview of key activities 26
7.2 Assessment and initial decision by the PoC 28
7.3 Assessment and incident confirmation by the ISIRT 30

8 Responses phase 31
8.1 Overview of key activities 31
8.2 Responses 32

9 Lessons learnt phase 40
9.1 Overview of key activities 40
9.2 Further information security forensic analysis 40
9.3 Identifying the lessons learnt 41
9.4 Identifying and making improvements to information security control implementation 42
9.5 Identifying and making improvements to information security risk assessment and management review results 42
9.6 Identifying and making improvements to the information security incident management scheme 42
9.7 Other improvements 43

Annex A (informative) **Cross reference table of ISO/IEC 27001 vs ISO/IEC 27035** 44

Annex B (informative) **Examples of information security incidents and their causes** 47

Annex C (informative) **Example approaches to the categorization and classification of information security events and incidents** 50

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 27035:2011

Annex D (informative) **Example information security event, yncident and vulnerability reports and forms** **62**

Annex E (informative) **Legal and regulatory aspects** **74**

Bibliography **76**

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27035:2011

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27035 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27035 cancels and replaces ISO/IEC TR 18044:2004, which has been technically revised.

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

Introduction

In general, 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 make information security ineffective and thus information security incidents possible. This can potentially have both direct and indirect adverse impacts on an organization's business operations. Further, 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 serious about information security 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 for the prevention and reduction of, and recovery from, impacts (for example in the support of crisis management areas);
- report information security vulnerabilities that have not yet been exploited to cause information security events and possibly information security incidents, and assess and deal with them appropriately;
- learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management.

This International Standard provides guidance on information security incident management in Clause 4 to Clause 9. These clauses consist of several subclauses, which include a detailed description of each phase.

The term ‘information security incident management’ is used in this International Standard to encompass the management of not just information security incidents but also information security vulnerabilities.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

INTERNATIONAL STANDARD ISO/IEC 27035:2011(E)

Information technology — Security techniques — Information security incident management

1 Scope

This International Standard provides a structured and planned approach to:

a) detect, report and assess information security incidents;

b) respond to and manage information security incidents;

c) detect, assess and manage information security vulnerabilities; and

d) continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

This International Standard provides guidance on information security incident management for large and medium-sized organizations. Smaller organizations can use a basic set of documents, processes and routines described in this International Standard, depending on their size and type of business in relation to the information security risk situation. It also provides guidance for external organizations providing information security incident management services.

2 Normative references

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

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

3 Terms 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 forensics
application of investigation and analysis techniques to capture, record and analyse information security incidents

3.2
information security incident response team
ISIRT
team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

NOTE The ISIRT as described in this International Standard is an organizational function that covers the process for information security incidents and is focused mainly on IT related incidents. Other common functions (with similar abbreviations) within the incident handling may have a slightly different scope and purpose. The following commonly used abbreviations have a meaning similar to that of ISIRT, though not exactly the same:

- CERT: A Computer Emergency Response Team mainly focuses on Information and Communications Technology (ICT) incidents. There may be other specific national definitions for CERT.
- CSIRT: A Computer Security Incident Response Team is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. These services are usually performed for a defined constituency, which could be a parent entity such as a corporation, governmental organization, or educational organization; a region or country; a research network; or a paid client.

3.3
information security event
identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant

[ISO/IEC 27000:2009]

3.4
information security incident
single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

[ISO/IEC 27000:2009]

4 Overview

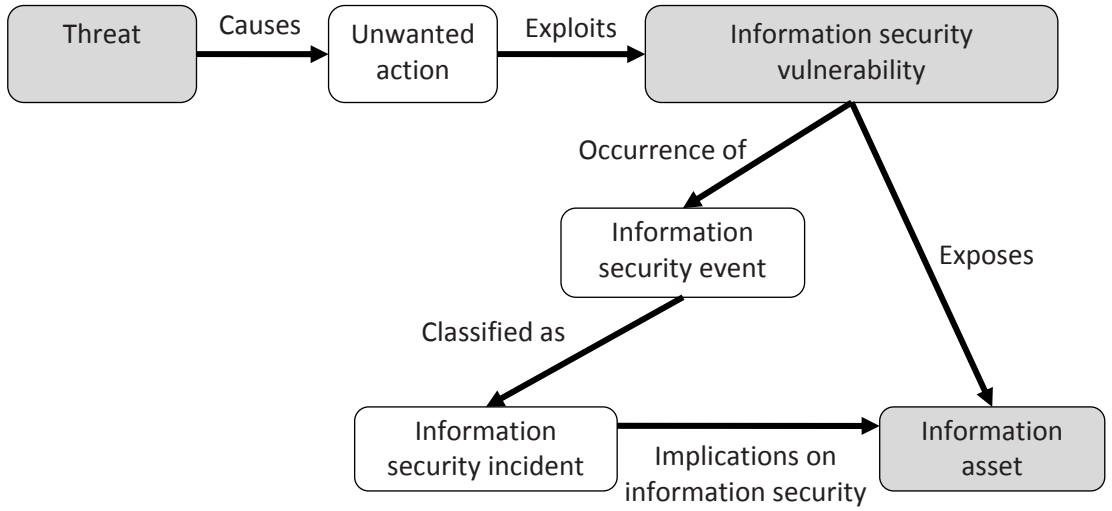
4.1 Basic concepts

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant. An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

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

A threat acts in unwanted ways to exploit the vulnerabilities (weaknesses) of information systems, services or networks, which is the occurrence of information security events and potentially causes unwanted incidents to information assets exposed by the vulnerabilities. Figure 1 shows this relationship of objects in an information security incident chain. The shaded objects are pre-existing, affected by the unshaded objects in the chain that results in an information security incident.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011



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

Figure 1 — The relationship of objects in an information security incident chain

4.2 Objectives

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 a business perspective, the prime objective is to avoid or contain the impact of information security incidents to reduce the direct and indirect costs caused by the incidents.

The primary steps to minimize the direct negative impact of information security incidents are the following:

- stop and contain,
- eradicate,
- analyse and report, and
- follow up.

The objectives of a structured well-planned approach are more refined and should ensure the following:

a) Information security events are detected and dealt with efficiently, in particular in identifying whether they need to be categorized and classified as information security incidents or not.

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 business operations are minimized by appropriate controls as part of the incident response, possibly in conjunction with relevant elements from a crisis management plan or plans.

d) Reported information security vulnerabilities are assessed and dealt with appropriately.

e) Lessons are learnt quickly from information security incidents, vulnerabilities and associated management. This is 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 scheme.

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 27035:2011

To help achieve this, organizations should ensure that information security incidents are documented in a consistent manner, using appropriate standards for incident categorization and classification, and sharing, so that metrics are created 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.

It is re-iterated that another objective associated with this International Standard is to provide guidance to organizations that aim to meet the requirements specified in ISO/IEC 27001 (and thus supported by guidance from ISO/IEC 27002). This includes information security incident management related requirements. A table that cross-references information security incident management related clauses in ISO/IEC 27001 and ISO/IEC 27002, and clauses in this International Standard is shown in Annex A.

4.3 Benefits of a structured approach

An organization using a structured approach to information security incident management will accrue significant benefits, which can be grouped under the followings.

a) Improving overall information security

A structured process for the 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 providing a means of preventing future similar information security incidents. Further, there will be benefits facilitated 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 27005:2008).

c) Strengthening the information security incident prevention focus

Using a structured approach to information security incident management helps to create a better focus on incident prevention within an organization, including identification methods of new threats and vulnerabilities. Analysis of incident related data would enable the identification of patterns and trends, thereby facilitating a more accurate focus on incident prevention and thus identification of appropriate actions to prevent incidents occurring.

d) Strengthening 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 a reactive mode, by responding to incidents as they occur and overlooking what activities are needed. This could prevent investigation activities from being directed to areas where they may be a higher priority where they are really needed and in the ideal priority.

e) Strengthening evidence

Clear incident investigation procedures can 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. It should be recognized, however, that there is a chance that the actions necessary to recover from an information security incident might jeopardize the integrity of any such collected evidence.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

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 within involved organizational units. Further, benefit will accrue for the information security incident management scheme itself, with the

- use of less skilled staff to identify and filter out the alarms of abnormality or anomaly,
- provision of better direction for the activities of skilled personnel, and
- engagement of skilled personnel only for those processes where their skills are needed and only at the stage of the process where their contribution is needed.

Another useful approach to control and optimize budget and resources, is to add time tracking to information security incident management to facilitate quantitative assessments of the organization's handling of information security incidents. It should, for example, 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 the

- 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 on frequencies of occurrence of the identified threat types.

The data collected on the adverse impacts on business operations from information security incidents will be useful in the business impact analysis. The data collected to identify the occurrence frequency of the various threat types will greatly aid the quality of the threat assessment. Similarly, the data collected on vulnerabilities will greatly aid the quality of future vulnerability assessments (for guidance on information security risk assessment and management, see ISO/IEC 27005:2008).

h) Providing enhanced information security awareness and training program material

A structured approach to information security incident management will provide focused information for information security awareness programs. This focused information will provide real examples demonstrating that information security incidents happen to real organizations. It will also be possible to demonstrate the benefits associated with the rapid availability of solution information. Furthermore, such awareness helps to reduce a mistake or panic/confusion by an individual in the event of an information security incident.

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

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

4.4 Adaptability

The guidance provided by this International Standard 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 kept in proportion to the following:

a) size, structure and business nature of an organization,

b) scope of any information security management system within which incidents are handled,

c) potential for loss through unprevented incidents arising, and

d) the goals of the business.

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 27035:2011

An organization using this International Standard should therefore adopt its guidance in due proportion to the scale and characteristics of their business.

4.5 Phases

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

- Plan and prepare,
- Detection and reporting,
- Assessment and decision,
- Responses, and
- Lessons learnt.

The first phase involves getting all that is required in place to operate successful information security incident management. The other four phases involve the operational use of information security incident management.

A high-level view of these phases is shown in Figure 2.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

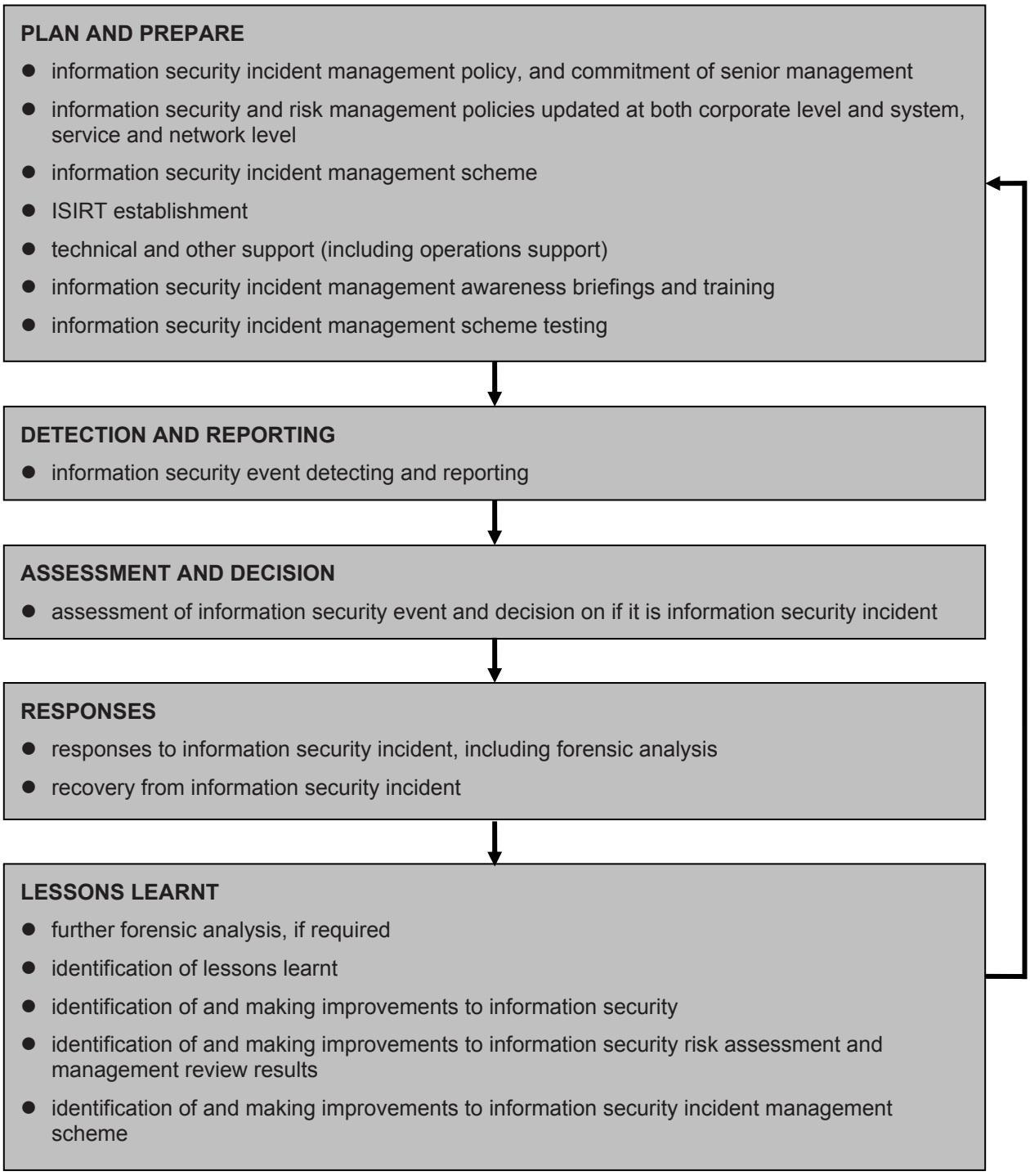


Figure 2 — Information security incident management phases

4.6 Examples of information security incidents

Information security incidents may be deliberate or accidental (e.g. caused by error or acts of nature), and may be caused by technical or physical means. Their consequences may include the disclosure, modification, destruction, or unavailability of information in an unauthorized manner, or the damage or theft of organizational assets. If unreported information security events are determined to be incidents, it becomes difficult to investigate the incidents and to take control in order to prevent recurrence.

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

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.

5 Plan and prepare phase

5.1 Overview of key activities

Effective information security incident management requires appropriate planning and preparation.For an efficient and effective information security event, incident and vulnerability management scheme to be put into operational use, an organization should complete a number of preparatory activities after the necessary planning. The organization should ensure that the activities of the plan and prepare phase include the following:

a) Activity to formulate and produce an information security event/incident/vulnerability management policy, and gaining senior management commitment to that policy. This should be preceded by an information security review of the organization's vulnerabilities, confirmation of the need for an information security incident management scheme, and identification of the benefits to the organization as a whole and to its departments (see Clause 5.2). Ensuring continued management commitment is vital for the acceptance of a structured approach to information security incident management. Personnel need to recognize an incident, know what to do and understand the benefits of the approach to the organization. Management needs to be supportive of the management scheme to ensure that the organization commits to resourcing and maintaining an incident response capability.

b) Activity to update information security and risk management policies at a corporate level and specific system, service and network levels. This should include reference to information security event, incident and vulnerability management. Policies need to be reviewed regularly in the context of output from the information security incident management scheme (see Clause 5.3).

c) Activity to define and document a detailed information security incident management scheme. Overall, the scheme documentation should encompass the forms, procedures, organizational elements and support tools for the detection and reporting of, assessment and decision making related to, making responses to, and learning lessons from, information security incidents. The topics for inclusion include:

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

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

   2) The information security event/incident/vulnerability forms:

      i) completed by the person reporting an information security event (i.e. not an information security incident management team member), with the information recorded in an information security event/incident/vulnerability database,

      ii) used by the information security incident management personnel to build on the initially reported information security event information and enable a running record of the incident assessments, etc. over time until the incident is fully resolved. At each stage, the update is recorded in the information security event/incident/vulnerability database. The completed information security event/incident/vulnerability database record is then used in post-incident resolution activities, and

      iii) completed by the person reporting an information security vulnerability (that has not yet been exploited to cause an information security event, and possibly an information security incident), with the information recorded in the information security event/incident/vulnerability database.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

It is recommended that these forms are electronic (e.g. in secure web page), linking directly to the electronic information security event/incident/vulnerability database. In today's world, the operation of a paper-based scheme would be time consuming. However, a paper-based scheme may be needed for a case where an electronic scheme can not be used.

NOTE Example forms are shown in Annex D.

3) The documented procedures and actions related to the use of the forms, i.e. associated with information security event, incident and vulnerability detection, with links to the normal procedures for the use of data and system, service and/or network backups and crisis management plans.

4) Operating procedures for the ISIRT, with documented processes and associated responsibilities, and the allocation of roles to designated persons to conduct various activities (an individual may be allocated more than one role, depending on the size, structure and business nature of an organization), for example including:

   i) shut down an affected system, service and/or network, in certain circumstances agreed by prior arrangement with the relevant IT and/or business management,

   ii) leave an affected system, service and/or network, connected and running,

   iii) monitor data flowing from, to and within an affected system, service and/or network,

   iv) activate normal back-up and crisis management procedures and actions in line with the system, service and/or network security policy,

   v) monitor and maintain the secure preservation of electronic evidence, in case it is required for legal prosecution or internal disciplinary action, and

   vi) communicate information security incident details to internal and external people or organizations.

   In some organizations, the scheme may be referred to as an information security incident response plan (see Clause 5.4).

d) Activity to establish the ISIRT, with an appropriate training program designed, developed and provided to its personnel. According to the size, structure and the nature of the business, an organization may have an ISIRT of a dedicated team, a virtual team, or a mix of the two options. A dedicated team may have virtual members identified in specific units/functions that should cooperate closely with the ISIRT during the resolution of an information security incident (ICT, legal, public relations, outsourcing companies, etc.). A virtual team may have a senior manager leading the team supported by groups of individuals specialized in particular topics, e.g. in the handling of malicious code attacks, who will be called upon depending on the type of incident concerned (see Clause 5.5).

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

f) Activity to establish, implement and operate technical and other support (including organizational) mechanisms for supporting the information security incident management scheme (and thus the work of the ISIRT), and in order to prevent information security incident occurrences or reduce the likelihood of occurrences of information security incidents (see Clause 5.6). Such mechanisms could include the following:

   1) Internal information security audit mechanisms to assess the security level and track vulnerable systems,

   2) Vulnerability management (including security updates and security patching of vulnerable systems).

   3) Technology watch to detect new kinds of threats and attacks.

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 27035:2011

4) Intrusion Detection Systems (for more details, see ISO/IEC 18043).

5) Network security devices, protections means and monitoring tools (for more details, see ISO/IEC 27033).

6) Anti-malicious code software.

7) Audit log records, and log monitoring software.

8) Documented responsibilities and operating procedures for the operations support team.

g) Activity to design and develop an information security event, incident and vulnerability management awareness and training program. All organizational personnel should be made aware through briefings and/or other mechanisms, of the existence of the information security event, incident and vulnerability management scheme, its benefits and how to report information security events and incidents (and vulnerabilities). In parallel, appropriate training should be provided to those personnel responsible for managing the information security event, incident and vulnerability management scheme, decision makers involved in determining whether information security events are incidents, and those individuals involved in the investigation of incidents. Awareness briefings and training sessions should be repeated later to accommodate changes in personnel (see Clause 5.7).

h) Activity to test the use of the information security incident management scheme, its processes and procedures. Tests should be organized periodically not only to test the scheme in a real situation, but also to verify how the ISIRT behaves under the pressure of a severe complex incident. Particular attention should be given to the creation of tests that focus on the evolving vulnerability, threat and risk scenarios (see Clause 5.8). The scheme should include standards that support information sharing, both within the organization and outside (if required by the organization). One of the benefits of sharing is the aggregation of data into useful metrics to aid strategic business decisions. Membership of a trusted information sharing community also provides early warning of attacks and should be encouraged in any information security incident management scheme and associated policy.

With this phase completed, organizations should be fully prepared to properly manage information security incidents. The following clauses describe each of the activities listed above, including the contents of each document required.

5.2 Information security incident management policy

5.2.1 Introduction

An organization should document its policy for managing information security events, incidents and vulnerabilities as a free-standing document, as part of its overall information security management system policy (see Clause 4.2.1 b) of ISO/IEC 27001:2005), or as part of its Information Security Policy (see Clause 5.1.1 of ISO/IEC 27002:2005). The size, structure and business nature of an organization and the extent of its information security incident management program are deciding factors in determining which of these options to adopt. Each organization should direct its information security incident management policy at every person having legitimate access to its information systems and related locations.

Before the policy is formulated, the organization should conduct an information security review highlighting its vulnerabilities, confirmation of the need for information security incident management, and identification of the benefits to the organization as a whole and to its departments.

5.2.2 Involved parties

An organization should ensure that its information security incident management policy is approved by a senior organization executive officer, with confirmed documented commitment from all of senior management. It should be made available for every employee and contractor, and should also be addressed in information security awareness briefings and training (see Clause 5.7).

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

5.2.3 Content

An organization should ensure that its information security incident management policy content addresses the following topics:

a) The importance of information security incident management to the organization, and senior management's commitment to it and the related scheme.

b) An overview of information security event detection, reporting and collection of relevant information, and how this information should be used to determine information security incidents.

   This overview should include a summary of possible types of information security events, how to report them, what to report, where and to whom, and how to handle entirely new types of information security events. It should also include a summary of information security vulnerability reporting and handling.

c) An overview of information security incident assessment, including a summary of who is responsible, what has to be done, notification, and escalation.

d) A summary of the activities that follow the confirmation that an information security event is an information security incident.

e) A reference to the need for ensuring that all information security incident management activities are properly logged for later analysis, and that continuous monitoring is conducted to ensure the secure preservation of electronic evidence, in case it is required for legal prosecution or internal disciplinary action.

f) Post information security incident resolution activities, including learning from and improving the process, following information security incidents.

g) An overview of information security vulnerability reporting and handling.

h) Details of where the scheme documentation, including procedures, is held.

i) An overview of the ISIRT, encompassing the following topics.

   1) The ISIRT organizational structure, and the identity of the ISIRT manager and other key personnel, including who is responsible for:

      i) briefing senior management on incidents,

      ii) dealing with enquiries, instigating follow up, etc., and

      iii) the link with the external organizations (when necessary).

   2) The information security management charter that specifies what the ISIRT is to do and the authority under which it does it. At a minimum, the charter should include a mission statement, a definition of the ISIRT's scope, and details of the ISIRT's board level sponsor and authority.

   3) The ISIRT mission statement that focuses on the team's core activities. In order to be considered an ISIRT, the team should support the assessing of, responding to, and managing of, information security incidents, to a successful conclusion. The goals and purposes of the team are especially important, and require clear, unambiguous definition.

   4) A definition of the scope of the ISIRT activities. Normally, the scope of an organization's ISIRT covers all of the organization's information systems, services and networks. In other cases, an organization may, for whatever reason, require the scope to be less than that, in which case it should be clearly documented what is in, and what is out of, scope.

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 27035:2011

5) Identification of a senior executive officer, board member or senior manager who has the authority to make decision on ISIRT and also establish the levels of authority for ISIRT. Knowing this helps all personnel in the organization to understand the background and set-up of the ISIRT, and it is vital information for building trust in the ISIRT. It should be noted that before this detail is promulgated, it should be checked from a legal perspective. In some circumstances, disclosure of a team's authority may expose it to claims of liability.

6) Links to organizations providing specific external support, such as forensics teams (see Clause 5.5.4).

j) An overview of the technical and other support mechanisms.

k) An overview of the information security incident management awareness and training program.

l) A summary of the legal and regulatory aspects that have to be addressed (for more details, see Annex E).

5.3 Information security incident management integration in other policies

5.3.1 Introduction

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

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

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

c) To ensure consistency across the various policies.

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

For guidance on information security risk assessment and management, see ISO/IEC 27005:2008.

5.3.2 Content

Each organization should update and maintain its corporate information security and risk management policies, and specific system, service or network information security policies. These policies need to refer to a corporate information security incident management policy and associated scheme explicitly.

a) The relevant sections should refer to the senior management commitment.

b) The relevant sections should outline the policy.

c) The relevant sections should outline scheme processes, and related infrastructure.

d) The relevant sections should outline requirements for detecting, reporting, assessing and managing information security events, incidents and vulnerabilities.

e) The relevant sections should clearly indicate those personnel responsible for authorizing and/or undertaking certain critical actions (e.g. taking an information system off-line or even shutting it down).

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

The policies should include the requirement that appropriate review mechanisms need to be established. These mechanisms need to ensure that information from the detection, monitoring and resolution of information security incidents and from dealing with reported information security vulnerabilities is used as input to ensure the continuing effectiveness of the corporate information security and risk management policies, and specific system, service or network information security policies.

5.4 Information security incident management scheme

5.4.1 Introduction

The aim of an information security incident management scheme is to provide detailed documentation describing the activities and procedures for dealing with information security events and incidents, and the communication of such events, incidents and vulnerabilities. The information security incident management scheme comes into effect whenever an information security event is detected, or an information security vulnerability is reported. Each organization should use the scheme as a guide for:

a) responding to information security events,

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

c) managing information security incidents to a conclusion,

d) responding to information security vulnerabilities,

e) identifying lessons learnt, and any improvements to the scheme and/or security in general that are required, and

f) making identified improvements.

5.4.2 Involved parties

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

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

b) assessing and responding to information security events and incidents, being involved in the post-incident resolution activities of learning, and improving information security and the information security incident management scheme itself (this is the responsibility of members of the PoC (Point of Contact), the ISIRT, management, public relations personnel and legal representatives), and

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

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

5.4.3 Content

Each organization should ensure that the content of the information security incident management scheme documentation includes the following:

a) An overview of the information security incident management policy.

b) An overview of the whole information security incident management scheme.

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 27035:2011

c) The detailed activities, procedures and information, associated with the following:

1) Plan and prepare

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

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

ii) A standard information security event/incident/vulnerability database structure, which is likely to provide the capability to compare results, improve alert information and enable a more accurate view of the threats to, and vulnerabilities of information systems

iii) Guidance for deciding whether escalation is required during each relevant process, and to whom, and associated procedures. Based on the guidance provided in the information security incident management scheme documentation, anyone assessing an information security event, incident or vulnerability should know in which circumstances it is necessary to escalate matters, and to whom it should be escalated to. In addition, there are unforeseen circumstances when this may be necessary. For example, a minor information security incident could evolve to a significant or a crisis situation if not handled properly or a minor information security incident not followed up in a week could become a major information security incident. The guidance should define information security event and incident types, escalation types and who may institute escalation.

iv) Procedures to be followed to ensure that all information security incident management activities are properly logged in the appropriate form, and that log analysis is conducted by designated personnel.

v) Procedures and mechanisms to ensure that the change control regime is maintained covering information security event, incident and vulnerability tracking and information security event/incident/vulnerability report updates, and updates to the scheme itself,

vi) Procedures for information security forensics analysis.

vii) Procedures and guidance on using Intrusion Detection Systems (IDS), ensuring that associated legal and regulatory aspects have been addressed. Guidance should include discussion of the advantages and disadvantages of undertaking attacker surveillance activities. Further information on IDS is contained in ISO/IEC 18043:2006.

viii) Guidance and procedures associated with the technical and organizational mechanisms that are established, implemented and operated in order to prevent information security incident occurrences and to reduce the likelihood of occurrences of information security incidents, and to deal with occurred information security incidents.

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

x) Procedures and specifications for the testing of the information security incident management scheme.

xi) The scheme of organizational structure for information security incident management.

xii) The terms of reference and responsibilities of the ISIRT as a whole, and of individual members.

xiii) Important contact information.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

2) Detection and reporting

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

   ii) Collecting the information on information security events.

   iii) Detecting and reporting on information security vulnerabilities.

   iv) Fully recording all information gathered in the information security incident management database.

3) Assessment and decision

   i) The PoC conducting assessments of information security events (including escalation as required), using the agreed information security event/incident classification scale (including determining the impacts of events based on the affected assets/services) and deciding whether events should be classified as information security incidents.

   ii) The ISIRT assessing information security events should confirm whether an event is an information security incident or not, and then another assessment should be conducted using the agreed information security event/incident classification scale to confirm the details of the event (potential incident) type and affected resource (categorization). This should be followed by decisions being made on how the confirmed information security incident should be dealt with, by whom and in what priority, as well as escalation levels.

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

   iv) Fully recording all assessment results and related decisions in the information security incident management database.

4) Responses

   i) Review by the ISIRT to determine if the information security incident is under control, and

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

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

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

   iii) Conducting information security forensics analysis, as required.

   iv) Escalation, on an as required basis.

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

   vi) Ensuring that electronic evidence is gathered and stored provably securely.

   vii) Ensuring that the change control regime is maintained, and thus that the information security event/incident/vulnerability database is kept up-to-date.

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

   ix) Dealing with information security vulnerabilities.

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 27035:2011

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

Each organization should ensure that the information security incident management scheme documentation allows for information security incident responses, both immediately and longer-term. All information security incidents should undergo an early assessment of the potential adverse impacts on business operations, both short and longer-term (for example, a major disaster could occur some time after an initial information security incident). Further, it should allow for some responses necessary for information security incidents that are completely unforeseen, where ad hoc controls are required. Even for this situation, organizations should encompass general guidelines in the scheme documentation on the steps that may be necessary.

5) Lessons learnt

i) Conducting further information security forensic analysis, as required.

ii) Identifying the lessons learnt from information security incidents and vulnerabilities.

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

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

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

vi) Updating the information security event/incident/vulnerability database.

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

5.4.4 Procedures

Before being able to commence operation of the information security incident management scheme, it is important that an organization has documented and checked that the procedures are available. Each procedure should indicate those groups or individuals responsible for its use and management, as appropriate from the PoC and/or the ISIRT. Such procedures should ensure that electronic evidence is gathered and stored securely, and that its secure preservation is continually monitored, in case it is required for legal prosecution or internal disciplinary action. Further, there should be documented procedures covering not just PoC and ISIRT activities, but those involved in information security forensic analysis and crisis activities – if not covered elsewhere, e.g. in a business continuity plan or a crisis management plan. The documented procedures should be entirely in line with the documented information security incident management policy and other information security incident management scheme documentation.

It is important to understand that not all procedures need be publicly available. For example, it is not necessary for all organizational personnel to understand the internal operation of an ISIRT in order to interact with it. The ISIRT should ensure that publicly available guidance, including information resulting from information security incident analysis, is in readily available form, e.g. on the organization's intranet. It may also be important to keep some details of the information security incident management scheme closely held to prevent an insider from tampering with the investigation process. For example, if a bank employee who is embezzling funds is aware of some details of the scheme, he or she may be able to better hide their activities from investigators or otherwise hamper the detection, investigation of and recovery from an information security incident.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

The content of operating procedures depends on a number of criteria, especially related to the nature of known potential information security events, incidents and vulnerabilities and the types on information system assets that might be involved and their environment. Thus, an operating procedure could be related to a particular type of incident or product (for example firewalls, databases, operating systems, applications) or to a specific product. Each operating procedure should clearly identify the steps to be undertaken and by whom. It should reflect experience from external (for example government and commercial ISIRTs or similar, and suppliers) as well as from internal sources.

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

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

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

c) pre-authorized delegation of decision making without normal approval process.

5.4.5 Trust

The ISIRT plays a crucial role for the overall information security of an organization. The ISIRT requires the collaboration of all organizational personnel to detect, resolve and investigate information security incidents. It is fundamental that the ISIRT is trusted by everybody, both internally and externally. Adoption of anonymity with regard to reporting information security vulnerabilities, events and incidents may be helpful to build trust.

An organization should ensure that its information security incident management scheme addresses situations where it is important to ensure the anonymity of the person or party that reports potential information security incidents or vulnerabilities under specific circumstances. Each organization should have provisions that clearly illustrate the expectation of anonymity, or lack thereof, for persons or parties reporting a potential information security incident or vulnerability. The ISIRT may need to obtain additional information not initially relayed by the person or party who reported the incident. Furthermore, important information about the information security incident or vulnerability itself may be derived from who detects it first.

Another approach that may be adopted by the ISIRT is to win users' trust through transparency and mature processes. The ISIRT should work to educate users, explain how the ISIRT works, how it protects confidentiality of information collected and how it manages users' event, incident and vulnerability reports.

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

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

5.4.6 Confidentiality

An information security incident management scheme may contain sensitive information, and people involved in addressing incidents and vulnerabilities may be required to handle sensitive information. An organization should ensure that the necessary processes are established to anonymize sensitive information and require personnel with access to sensitive information to sign confidentiality agreements.. If information security events/incidents/vulnerabilities are logged via a generalized problem management system, sensitive details may have to be omitted. Additionally, an organization should ensure that the information security incident management scheme makes provision for controlling the communication of incidents and vulnerabilities to external parties, including the media, business partners, customers, law enforcement organizations, and the general public.

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 27035:2011

5.5 Establishment of the ISIRT

5.5.1 Introduction

The aim of establishing the ISIRT is to provide the organization with appropriate capability for assessing, responding to and learning from information security incidents, and providing the necessary co-ordination, management, feedback and communication. An ISIRT contributes to the reduction in physical and monetary damage, as well as the reduction of the damage to the organization's reputation that is sometimes associated with information security incidents.

5.5.2 Members and structure

The size, structure and composition of an ISIRT should be appropriate for the size, structure, and the business nature of the organization. Although the ISIRT may constitute an isolated team or department, members may share other duties, which encourage the input of members from a range of areas within the organization. An organization should evaluate if it requires a dedicated team, a virtual team, or a mix of the two. The number of incidents and the activities performed by the ISIRT should guide the organization in this choice.

The ISIRT goes through different maturity stages and often adjustments to the organizational model are adopted based on the specific scenario faced by the organization. Whenever justified, it is recommended to have a permanent team led by a senior manager. Virtual ISIRTs teams may be led by a senior manager. The senior manager should be supported by individuals who are specialized in particular topics, for example in handling malicious code attacks, which are called upon depending on the type of information security incident concerned. Depending on the size, structure and business nature of an organization, a member may also fulfil more than one role within the ISIRT. The ISIRT may comprise individuals from different parts of the organization (e.g. business operations, ICT, audit, human resources and marketing). This also applies to permanent ISIRTs; even in case of dedicated personnel, the ISIRT always requires support from other departments.

Team members should be accessible for contact, so the names and contact details of each member and their backup members should be available within the organization. The necessary details should be clearly indicated in the information security incident management scheme documentation, including any procedural documents, and the reporting forms, but not in policy statements.

The ISIRT manager should usually have a separate line of reporting to senior management, separate from normal business operations. He/she should have delegated authority to make immediate decisions on how to deal with an incident, and should ensure that all ISIRT members have the required knowledge and skills levels, and that these continue to be maintained. The ISIRT manager should assign investigation of each incident to the most appropriate member of his/her team, with each incident assigned a named manager.

5.5.3 Relationship with other parts of the organization

The ISIRT should have the responsibility for ensuring that incidents are resolved, and in this context the ISIRT manager and members of his/her team should have a degree of authority to take the necessary actions deemed appropriate in response to information security incidents. However, actions that may have adverse effects on the overall organization, either financially or in terms of reputation, should be agreed with senior management. For this reason, it is essential that the information security incident management policy and scheme details the appropriate authority to which the ISIRT manager reports serious information security incidents.

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

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011

5.5.4 Relationship with external interested parties

Organizations should establish relationships between the ISIRT and appropriate external interested parties. External interested parties may include the following:

a) contracted external support personnel,

b) external organizations' ISIRTs ,

c) managed service providers, including tellecommunication service providers, ISPs and suppliers,

d) law enforcement organizations,

e) emergency authorities,

f) appropriate government organizations,

g) legal personnel,

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

i) business partners,

j) customers, and

k) the general public.

5.6 Technical and other support (including operational support)

To ensure that quick and effective responses to information security incidents can be achieved, an organization should acquire, prepare and test all necessary technical and other support means. This includes the following:

a) access to details of the organization's assets with an up-to-date asset register and information on their links to business functions,

b) access to the documented procedures related to crisis management,

c) documented and promulgated communications processes,

d) the use of an information security event/incident/vulnerability database and the technical means to populate and update the database quickly, analyze its information and facilitate responses (in some instances manual records may be required by an organization), with the database kept provably secure,

e) facilities for information security forensics evidence collection and analysis, and

f) adequate crisis management arrangements for the information security event/incident/vulnerability database (for guidance on business continuity management see ISO/IEC 27031).

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

g) quick acquisition of information security event/incident/vulnerability reports,

h) notification of previously selected external personnel by appropriate means (for example electronic mail, fax or telephone), thus requiring the maintenance of a reliable, readily accessible contact database (including paper and other backups), and the facility to transmit information to individuals in a secure fashion where appropriate,

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27035:2011