TECHNICAL REPORT

ISO/IEC TR 18044

First edition
2004-10-15

Information technology — Security techniques — Information security incident management

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

Reference number
ISO/IEC TR 18044:2004(E)

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

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.

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.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/IEC TR 18044, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

No typical information security policies or safeguards will guarantee total protection of information, information systems, services or networks. After safeguards have been implemented, residual weaknesses are likely to remain that may make information security ineffective and thus information security incidents possible, potentially with both direct and indirect adverse impacts on an organization's business operations. Further, inevitably new previously unidentified threats will occur. Insufficient preparation by an organization to deal with such incidents will make any actual response less effective, and potentially increase the degree of potential adverse business impact. Therefore it is essential for any organization that is 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 by the activation of appropriate safeguards for the prevention and reduction of, and recovery from, impacts (for example in the support and business continuity planning areas),
- learn from information security incidents, institute preventive safeguards, and, over time, make improvements to the overall approach to information security incident management.

Information technology — Security techniques — Information security incident management

1 Scope

This Type 3 Technical Report (TR) provides advice and guidance on information security incident management for information security managers, and information system, service and network managers.

This TR contains 11 clauses and is organized in the following manner. Clause 1 describes the scope and is followed by a list of references in Clause 2 and terms and definitions in Clause 3. Clause 4 provides some background to information security incident management, and that is followed by a summary of the benefits and key issues in Clause 5. Examples of information security incidents and their causes are then provided in Clause 6. The planning and preparation for information security incident management, including document production, is then described in Clause 7. The operational use of the information security incident management scheme is described in Clause 8. The review phase of information security management, including the identification of lessons learnt and improvements to security and the information security incident management scheme, is described in Clause 9. The improvement phase, i.e. making identified improvements to security and the information security incident management scheme, is described in Clause 10. Finally, the TR concludes with a short summary in Clause 11. Annex A contains example information security event and incident report forms, and Annex B contains some example outline guidelines for assessing the adverse consequences of information security incidents, for inclusion in the reporting forms. The Annexes are followed by the Bibliography.

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 13335-1:2004, *IT security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 17799:2000, *Information technology — Code of practice for information security management*

3 Terms and Definitions

For the purposes of this document the terms and definitions given in ISO/IEC 13335-1, ISO/IEC 17799 and the following apply.

3.1 Business continuity planning

Business continuity planning is the process to ensure that recovery of operations will be assured should any unexpected or unwanted incident occur that is capable of negatively impacting the continuity of essential business functions and supporting elements. The process should also ensure that recovery is achieved in the required priorities and timescales, and subsequently all business functions and supporting elements will be recovered back to normal.

The key elements of this process need to ensure that the necessary plans and facilities are put in place, and tested, and that they encompass information, business processes, information systems and services, voice and data communications, people and physical facilities.

3.2 Information security event

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 safeguards, or a previously unknown situation that may be security relevant.

3.3 Information security incident

An information security incident is indicated by 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. (Examples of information security incidents are shown in Clause 6.)

3.4 ISIRT (Information Security Incident Response Team)

An ISIRT is a team of appropriately skilled and trusted members of the organization, which will handle information security incidents during their lifecycle. At times this team may be supplemented by external experts, for example from a recognized computer incident response team or Computer Emergency Response Team (CERT).

3.5 Other

Also see the definitions in ISO/IEC JTC1 SC27 SD6, Glossary.

4 Background

4.1 Objectives

As a key part of any organization's overall information security strategy, it is essential to have in place a structured well-planned approach to the management of information security incidents.

The objectives of this approach are to ensure that:

- information security events can be detected and dealt with efficiently, in particular in identifying whether they need to be categorized as information security incidents or not,[1]
- identified information security incidents are assessed and responded to in the most appropriate and efficient manner,
- the adverse impacts of information security incidents on the organization and its business operations can be minimized by appropriate safeguards as part of the incident response, possibly in conjunction with relevant elements from a business continuity plan or plans,
- lessons can be quickly learnt from information security incidents and their management. This is to increase the chances of preventing future information security incidents occurring, improve the implementation and use of information security safeguards, and improve the overall information security incident management scheme.

4.2 Processes

To achieve the objectives outlined in Clause 4.1, information security incident management consists of four distinct processes:

- Plan and Prepare,
- Use,
- Review,
- Improve.

[1] It should be noted that information security events could be the result of accidental or intentional attempts to breach information security safeguards, but in most cases an information security event alone does not imply that an attempt has really been successful and therefore doesn't need to have any implications on confidentiality, integrity and/or availability, i.e. not all information security events will be categorized as information security incidents.

(It should be noted that these processes are similar to those reflected in the "Plan, Do, Check and Act' model in IS 9000 and IS 14000.)

A high level view of these processes is shown in Figure 1 below.

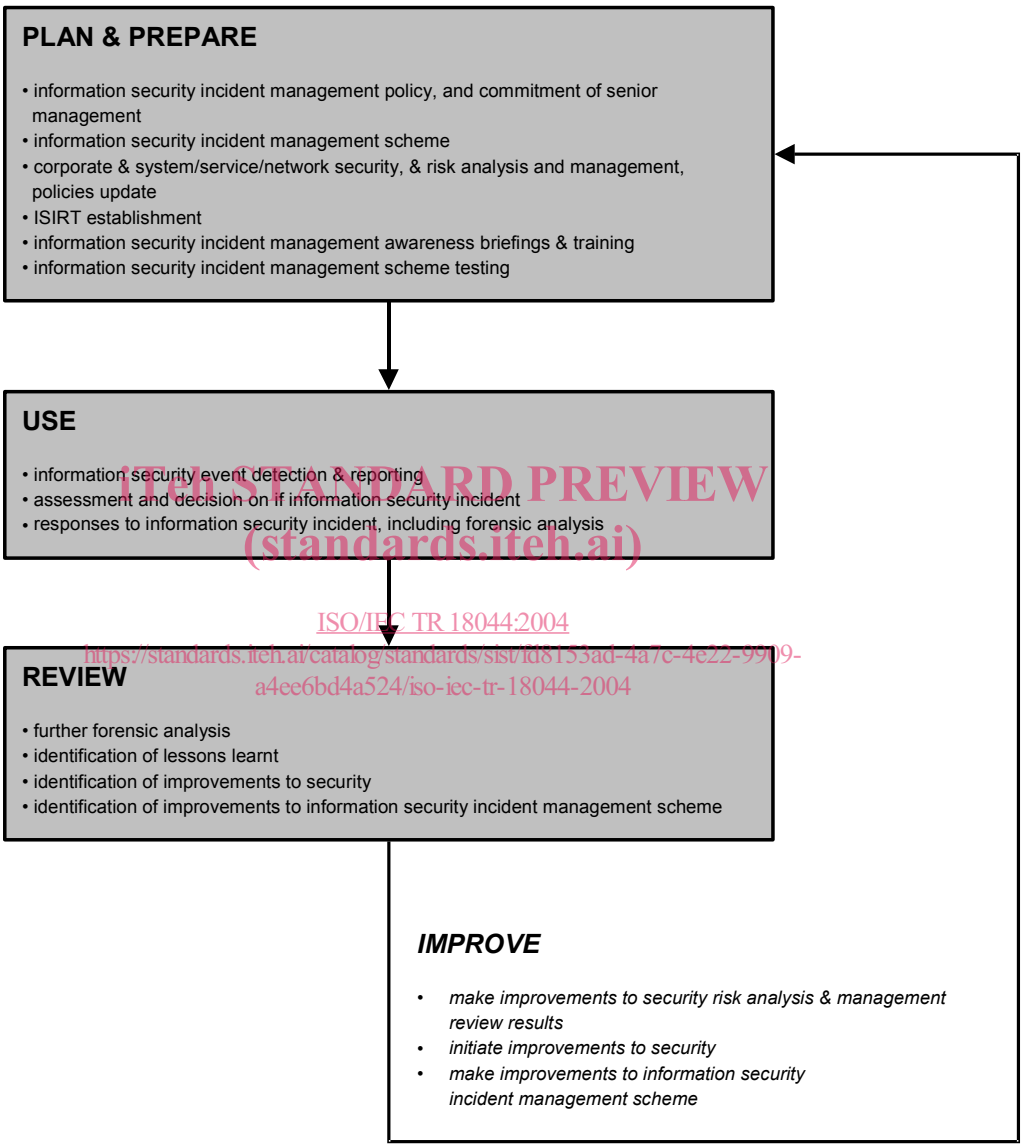

Figure 1- Information Security Incident Management Processes

4.2.1 Plan and Prepare

Effective information security incident management requires appropriate planning and preparation. For responses to information security incidents to be effective, the following actions are necessary:

- develop and document an information security incident management policy and gain visible commitment to that policy from all key stakeholders, particularly senior management,
- develop and comprehensively document an information security incident management scheme to support the information security incident management policy. Forms, procedures and support tools, for the detection, reporting, assessment and response to information security incidents, and details of the incident severity scale[2], should be encompassed within scheme documentation. (It should be noted that in some organizations, the scheme may be referred to as an information security incident response plan.),
- update information security and risk management policies at all levels, i.e. corporate-wide and for each system, service and network, with references to the information security incident management scheme,
- establish an appropriate information security incident management organizational structure, i.e. the Information Security Incident Response Team (ISIRT), with defined roles and responsibilities allocated to personnel who are available to enable an adequate response to all known types of information security incident. Within most organizations the ISIRT will be a virtual team, with 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,
- make all organizational personnel aware through briefings and/or other mechanisms, of the existence of the information security incident management scheme, its benefits and how to report an information security event. Appropriate training should be provided to those personnel responsible for managing the information security incident management scheme, decision makers involved in determining whether information security events are incidents, and those individuals involved in the investigation of incidents,
- thoroughly test the information security incident management scheme.

The Plan and Prepare phase is further described in Clause 7.

4.2.2 Use

The following processes are necessary to make use of an information security incident management scheme:

- detecting and reporting the occurrence of information security events (by human or automatic means),
- collecting information associated with information security events, and assessing that information to determine what events are to be categorized as information security incidents,
- making responses to information security incidents:
  - immediately, in real-time or in near real-time,
  - where information security incidents are under control, conducting activities that may be required in slower time (for example, in facilitating full recovery from a disaster),
  - if information security incidents are not under control, instigating ‘crisis’ activities (for example, calling the fire brigade/department or activating a business continuity plan),
  - communicating the existence of information security incidents and any relevant details thereof to internal and external people and/or organizations. (This could include escalating for further assessments and/or decisions as required.),

[2] An incident severity scale to be used to ‘grade’ incidents should be established. This scale could, for example, be ‘major’ and ‘minor’, with, in any event, the decision based on the actual or projected adverse impacts on the organization’s business operations.

- forensic analysis,
- properly logging all activities and decisions for further analysis,
- closing incidents on resolution.

The Use phase is further described in Clause 8.

4.2.3 Review

After information security incidents have been resolved/closed, the following review activities are necessary:

- conducting further forensic analysis, as required,
- identifying the lessons learnt from information security incidents,
- identifying improvements to information security safeguard implementation, as result of the lessons learnt, whether from one information security incident or many,
- identifying improvements to the information security incident management scheme as a whole, as a result of lessons learnt from quality assurance reviews of the approach (for example, from review of the effectiveness of the processes, procedures, the reporting forms and/or the organizational structure).

The Review phase is further described in Clause 9.

4.2.4 Improve

It is emphasized that the information security incident management processes are iterative, with regular improvements made to a number of information security elements over time. These improvements will be proposed on the basis of reviews of the data on information security incidents and the responses to them, as well as trends over time. This will include:

- revising the organization's existing information security risk analysis and management review results,
- making improvements to the information security incident management scheme and its documentation,
- initiating improvements to security, that may encompass the implementation of new and/or updated information security safeguards.

The Improve phase is further described in Clause 10.

5 Benefits and Key Issues

This clause provides information on the:

- benefits to be obtained from a good information security incident management scheme,
- key issues that need to be addressed to convince senior corporate management and those personnel who will report to and receive feedback from the scheme.

5.1 Benefits

Any organization using a structured approach to information security incident management may accrue significant benefits, which can be grouped under:

- improving information security,

- reducing adverse business impacts, for example disruption and financial loss, caused as a consequence of information security incidents,
- strengthening the information security incident prevention focus,
- strengthening of prioritization and evidence,
- contributing to budget and resource justifications,
- improving updates to risk analysis and management results,
- providing enhanced information security awareness and training program material,
- providing input to information security policy and related documentation reviews.

Each of these topics is introduced below.

5.1.1 Improving Security

A structured process for detecting, reporting, assessing and managing information security events and incidents enables rapid identification and response to any information security event or incident, thus improving overall security by helping to quickly identify and implement a consistent solution, providing a means of preventing future similar information security incidents.

5.1.2 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.

5.1.3 Strengthening Incident Prevention Focus

Using a structured approach to information security incident management can help to create a better focus on incident prevention within an organization. Analysis of incident related data will 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.

5.1.4 Strengthening of Prioritization and Evidence

A structured approach to information security incident management will provide a solid basis for prioritization when conducting information security incident investigations.

If there are no clear procedures, there is a risk that investigation activities could be conducted in a reactive mode, responding to incidents as they occur and to the “loudest voice” of related management. This could prevent investigation activities from being directed where they are really needed and in the ideal priority.

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.

5.1.5 Budget and Resources

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 false alarms,
- provision of better direction for the activities of skilled personnel,

- 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.

In addition, a structured approach to information security incident management can include 'time stamping' so that it is possible to make 'quantitative' assessments of the organization's handling of security incidents. It should, for example, be possible to provide information on how long it takes to resolve incidents of different priorities and on different platforms. If there are bottlenecks in the information security incident management process, these should also be identifiable.

5.1.6 Information Security Risk Analysis and Management

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

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

- provision of data on frequencies of occurrence of the identified threat types.

The data gained on the adverse impacts on business operations from information security incidents will be useful in the business impact analysis. The data gained identifying the occurrence frequency of the various threat types will greatly aid the quality of the threat assessment. Similarly, the data gained on vulnerabilities will greatly aid the quality of future vulnerability assessments.

This data will greatly improve information security risk analysis and management review results.

5.1.7 Information Security Awareness

A structured approach to information security incident management will provide focused information for information security awareness programs. This focused information will provide a source of real example information capable of demonstrating that information security incidents do actually happen to the organization, and not always "to somebody else". 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.

5.1.8 Input to Information Security Policy Review

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 organization-wide and for individual systems, services and networks.

5.2 Key Issues

Feedback on the way information security incidents have been managed will assist personnel to ensure that their work remains focused on the real risks to the organization's systems, services and networks. This important feedback cannot be as effectively provided through dealing with information security incidents as they occur on an ad hoc basis. It can be more effectively provided through the use of a structured well-designed information security incident management scheme that uses a common framework for all parts of the organization. This framework should continually enable more comprehensive results to be produced from the scheme, and allow a solid base for the rapid identification of possible information security incident conditions to be represented before an information security incident occurs, sometimes called "alerts".

The management and audit of the information security management scheme should provide the basis for the trust necessary to facilitate widespread participation, and to allay any concerns about the preservation of anonymity, security and the availability of useful results. For example, management and operations personnel need to be confident that "alerts" will give timely, relevant, accurate, concise and complete information.

Organizations need to avoid potential problems in implementing information security incident management schemes, such a lack of useful results and concerns about privacy related issues. It is necessary to convince stakeholders that steps have been taken to prevent such problems occurring.

Thus, a number of key issues should be addressed to achieve a good information security incident management scheme, including:

- management commitment,
- awareness,
- legal and regulatory aspects,
- operational efficiency and quality,
- anonymity,
- confidentiality,
- credible operations,
- typology.

Each of these issues is discussed below.

5.2.1 Management Commitment

Ensuring continued management commitment is vital for the acceptance of a structured approach to information security incident management. Personnel need to recognize an incident and know what to do, and even understand the broad benefits of the approach to the organization. However, unless management is supportive, little will happen. The idea needs to be sold to management so that the organization commits to resourcing and maintaining an incident response capability.

5.2.2 Awareness

Another important issue for the acceptance of a structured approach to information security incident management is that of awareness. Whilst users should be required to participate, if they are not aware of how they and their part of the organization may benefit from participating in a structured approach to information security incident management, they are less likely to participate effectively in its operation.

Any information security incident management scheme should be accompanied with an awareness program definition document that includes details of the:

- benefits to be derived from the structured approach to information security incident management, both to the organization and to its personnel,
- incident information held in, and the outputs from, the information security event/incident database,
- strategy and mechanisms for an awareness program, that, depending on the organization, could be standalone or part of a broader information security awareness program.

5.2.3 Legal and Regulatory Aspects

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

- **Adequate Data Protection and Privacy of Personal Information is Provided.** In those countries where specific legislation exists that covers data confidentiality and integrity, it is often restricted to the control of personal data. As information security incidents need to be typically attributable to an individual, information of a personal nature may therefore need to be recorded and managed accordingly. A structured approach to information security incident management therefore needs to take into account the appropriate privacy protection. This may include:

- those individuals with access to the personal data should, so far as is practical, not personally know the person(s) being investigated;
- non-disclosure agreements should be signed by those individuals with access to the personal data prior to them being allowed access to it;
- information should only be used for the express purpose for which it has been obtained, i.e. for information security incident investigation.

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

- **Safeguards are in place to Ensure Fulfillment of Commercial Contractual Obligations.** Where there are binding requirements on the provision of an information security incident management service, for example covering required response times, an organization should ensure that appropriate information security is provided to ensure that such obligations can be met in all circumstances. (Related to this, if an organization contracts with an external party for support (see Clause 7.5.4), for example a CERT, then it should be ensured that all requirements, including response times, are included in the contract with the external party.)

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

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

- **Contracts with External Support Personnel cover all Required Aspects.** Contracts with any external support personnel, for example from a CERT, should be thoroughly checked regarding waivers on liability, non-disclosure, service availability, and the implications of incorrect advice.

- **Non-Disclosure Agreements are Enforceable**. Information security incident management team members may be required to sign non-disclosure agreements both when starting and leaving employment. In some countries, having signed non-disclosure agreements may not be effective in law; this should be checked.

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

- **Liability Aspects are Clear.** The issues of potential liability, and related required safeguards to be in place, need to be clarified. Examples of events which may have associated liability issues are:
  - if an incident could affect another organization (for example, disclosure of shared information), and it is not notified in time and the other organization suffers an adverse impact,
  - if a new vulnerability in a product is discovered, and the vendor is not notified and a major related incident occurs later with major impact on one or more other organizations,
  - a report is not made where, in the particular country, organizations are required to report to or generate archives for law enforcement agencies regarding any case that may involve a serious crime, or penetration of a sensitive government system or part of the critical national infrastructure,
  - information is disclosed that seems to indicate that someone, or an organization, may be involved in an attack. This could damage the reputation and business of the person or organization involved.