TECHNICAL REPORT

ISO/IEC TR 27008

First edition
2011-10-15

Information technology — Security techniques — Guidelines for auditors on information security controls

Technologies de l'information — Techniques de sécurité — Lignes directrices pour les auditeurs des contrôles de sécurité de l'information

Reference number
ISO/IEC TR 27008:2011(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, 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), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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 TR 27008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This Technical Report supports the Information Security Management System (ISMS) risk management process defined within ISO/IEC 27001 and ISO/IEC 27005, and the controls included in ISO/IEC 27002.

This Technical Report provides guidance on reviewing an organization's information security controls, e.g. in the organization, business processes and system environment, including technical compliance checking.

Please refer to ISO/IEC 27007 for advice on auditing the management systems elements, and ISO/IEC 27006 regarding ISMS compliance reviewing for certification purposes.

Information technology — Security techniques — Guidelines for auditors on information security controls

1 Scope

This Technical Report provides guidance on reviewing the implementation and operation of controls, including technical compliance checking of information system controls, in compliance with an organization's established information security standards.

This Technical Report is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations conducting information security reviews and technical compliance checks. This Technical Report is not intended for management systems audits.

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 27000:2009, *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
review object
specific item being reviewed

3.2
review objective
statement describing what is to be achieved as a result of a review

3.3
security implementation standard
document specifying authorized ways for realizing security

4 Structure of this Technical Report

This Technical Report contains a description of the information security control review process including technical compliance checking.

Background information is provided in Clause 5.

Clause 6 provides an overview of information security control reviews.

The review methods are presented in Clause 7 and activities in Clause 8.

Technical compliance checking is supported by Annex A, and initial information gathering by Annex B

5 Background

An organization's information security controls should be selected based on the result of a risk assessment, as part of an information security risk management process, in order to reduce its risk to an acceptable level. However, organizations deciding not to implement an ISMS, may chose other means of selecting, implementing and maintaining information security controls.

Typically parts of an organization's information security controls are realized by the implementation of technical information security controls, e g. when information assets include information systems.

An organization's technical security controls should be defined, documented, implemented and maintained according to technical information security standards. As time passes, internal factors such as amendments of information systems, configurations of security functions and changes of surrounding information systems, and external factors such as advance of attack skills may negatively affect the effectiveness of information security controls and ultimately the organization's information security standards. Organizations should have a rigorous program for information security change control. Organizations should regularly review whether security implementation standards are appropriately implemented and operated. Technical compliance checking is included in ISO/IEC 27002:2005 as one of the controls, which is performed either manually and/or by technical reviews with the assistance of automated tools. It may be performed by a role not involved in executing the control, e.g. a system owner, or by staff in charge of the specific controls, or by internal or external information security experts including IT auditors.

The review output of technical compliance checking will account for the actual extent of technical compliance with information security implementation standards of the organization. This evidence provides assurance when the status of technical controls comply with information security standards, or otherwise the basis for improvements. The audit reporting chain should be clearly established at the outset of the review and the integrity of the reporting process should be assured. Steps should be taken to ensure that:

- relevant accountable parties receive, directly from the information security control review auditors, an unaltered copy of the report,
- inappropriate or unauthorized parties do not receive a copy of the report from the information security control review auditors, and
- the information security control review auditors are permitted to carry out their work without hindrance.

Information security control reviews, and technical compliance checking in particular, may help an organization to:

- identify and understand the extent of potential problems or shortfalls in the organization's implementation and operation of information security controls, information security standards and, consequently, technical information security controls,
- identify and understand the potential organizational impacts of inadequately mitigated information security threats and vulnerabilities,
- prioritize information security risk mitigation activities,
- confirm that previously identified or emergent information security weaknesses or deficiencies have been adequately addressed, and/or
- support budgetary decisions within the investment process and other management decisions relating to improvement of organization's information security management.

This Technical Report focuses on reviews of information security controls, including checking of technical compliance, against an information security implementation standard, which is established by the organization. It does not intend to provide any specific guidance on compliance checking regarding measurement, risk assessment or audit of an ISMS as specified in ISO/IEC 27004, 27005 or 27007 respectively.

The use of this document as a starting point in the process of defining procedures for reviewing information security controls promotes a more consistent level of information security within the organization. It offers the needed flexibility to customize the review based on business missions and goals, organizational policies and

requirements, known threat and vulnerability information, operational considerations, information system and platform dependencies, and risk appetite.

NOTE ISO Guide 73 defines risk appetite as the amount and type of risk that an organization is prepared to pursue, retain or take.

6 Overview of information security control reviews

6.1 Review process

When an individual information security-related review commences, the auditors associated with this review, information security control review auditors, normally start by gathering preliminary information, reviewing the planned scope of work, liaising with managers and other contacts in the applicable parts of the organization and expanding the review risk assessment to develop review documentation to guide the actual review work. For efficient reviews the assigned information security control review auditors need to be well prepared, both on the control side as well as on the testing side (e.g. operation of applicable tools, technical aim of the test). At this level, elements of the review work may also be prioritized according to the perceived risks but they may also be planned to follow a particular business process or system, or simply be designed to cover all areas of the review scope in sequence.

Preliminary information can come from a variety of sources:

- books, Internet searches, technical manuals, standards and other general background research into common risks and controls in this area, conferences, workshops, seminars or forums,
- results of prior reviews, tests, and assessments, whether partially or fully aligned with the present review scope and whether or not conducted by information security control review auditors (e.g. pre-release security tests conducted by information security professionals can provide a wealth of knowledge on the security of major application systems),
- information on relevant information security incidents, near-misses, support issues and changes, gathered from IT Help Desk, IT Change Management, IT Incident Management processes and similar sources, and
- generic review checklists and articles by information security control review auditors or information security professionals with expertise in this area.

It may be appropriate to review the planned review scope in light of the preliminary information, especially if the review plan that originally scoped the review was prepared many months beforehand. For example, other reviews may have uncovered concerns that are worth investigating in more depth, or conversely may have increased assurance in some areas, allowing the present work to focus elsewhere.

Liaising with managers and review contacts at this early stage is an important activity. At the end of the review process, these people will need to understand the review findings in order to respond positively to the review report. Empathy, mutual respect and making the effort to explain the review process significantly improve the quality and impact of the result.

While individuals vary in the manner in which they document their work, many review functions utilize standardized review processes supported by document templates for working papers such as review checklists, internal control questionnaires, testing schedules, risk-control matrices *etc*.

The review checklist (or similar) is a key document for several reasons:

- it lays out the planned areas of review work, possibly to the level of detailing individual review tests and anticipated/ideal findings,
- it provides structure for the work, helping to ensure that the planned scope is adequately covered,
- the analysis necessary to generate the checklist in the first place prepares the information security control review auditors for the review fieldwork that follows, while completing the checklist as the review progresses starts the analytical process from which the review report will be derived,
- it provides the framework in which to record the results of review pre-work and fieldwork and, for example, a place to reference and comment on review evidence gathered,
- it can be reviewed by audit management or other information security control review auditors as part of the review quality assurance process, and

- once fully completed, it (along with the review evidence) constitutes a reasonably detailed historical record of the review work as conducted and the findings arising that may be required to substantiate or support the review report, inform management and/or help with planning future reviews.

Information security auditors should be wary of simply using generic review checklists written by others as, aside from perhaps saving time, this would probably negate several of the benefits noted above. [This tends to be less of an issue with straightforward compliance or certification reviews since the requirements that have to be met are generally quite explicit.]

The bulk of review fieldwork consists of a series of tests conducted by the auditors, or at their requests, to gather review evidence and to review it, often by comparison to anticipated or expected results themselves derived from relevant compliance obligations, standards or a more general appreciation of good practices. For instance, one test within an information security review examining malware controls might check whether all applicable computing platforms have suitable antivirus software. Review tests such as this often use sampling techniques since there are seldom sufficient review resources to test exhaustively. Sampling practices vary between auditors and situations, and can include random selection, stratified selection and other more sophisticated statistical sampling techniques (*e.g.* taking additional samples if the initial results are unsatisfactory, in order to substantiate the extent of a control weakness). As a general rule, more exhaustive testing is possible where evidence can be gathered and tested electronically, for example using SQL queries against a database of review evidence collated from systems or asset management databases. The audit sampling approach should be guided, at least in part, by the risks attached to the area of operations being audited.

Evidence collected in the course of the review should normally be noted, referenced or inventoried in the review working papers. Along with review analysis, findings, recommendations and reports, review evidence need to be adequately protected by the information security control review auditors, particularly as some is likely to be highly sensitive and/or valuable. Data extracted from production databases for review purposes, for example, should be secured to the same extent as those databases through the use of access controls, encryption *etc*. Automated review tools, queries, utility/data extract programs *etc*. should be tightly controlled. Similarly, printouts made by or provided to the information security control review auditors should generally be physically secured under lock and key to prevent unauthorized disclosure or modification. In the case of particularly sensitive reviews, the risks and hence necessary information security controls should be identified and prepared at an early stage of the review.

Having completed the review checklist, conducted a series of review tests and gathered sufficient review evidence, the information security control review auditors should be in a position to examine the evidence, determine the extent to which information security risks have been treated, and review the potential impact of any residual risks. At this stage, a review report of some form is normally drafted, quality reviewed within the review function and discussed with management, particularly management of the business units, departments, functions or teams most directly reviewed and possibly also other implicated parts of the organization.

Audit managers should dispassionately review evidence to check that:

- there is sufficient review evidence to provide a factual basis supporting all of the review findings, and
- all findings and recommendations are relevant with regards to the review scope and non-essential matters are excluded.

If further review work is planned for findings this should be marked in the report.

As with review planning, the analysis process is essentially risk-based albeit better informed by evidence gathered during the review fieldwork. Whereas straightforward compliance reviewing can usually generate a series of relatively simple pass/fail results with largely self-evident recommendations, information security reviews often generate matters requiring management thought and discussion before deciding on what actions (if any) are appropriate. In some cases, management may elect to accept certain risks identified by information security reviews, and in others they may decide not to undertake the review recommendations exactly as stated: this is management's right but they also carry accountability for their decisions. In this sense, information security control review auditors perform an advisory, non-operational role, albeit they carry significant influence and are backed by sound review practices and factual evidence.

Information security control review auditors should provide the organization subject to the review with reasonable assurance that the information security activities (not all will implement a management system) achieve the set goals. A review should provide a statement of difference between the reality and a reference. When the reference is an internal policy, the policy should be clear enough to serve as a reference. The criteria listed in Annex B may be considered to ensure this. Information security control review auditors should

then consider internal policies and procedures within the review scope. Missing relevant criteria may still be applied informally within the organization. The absence of criteria identified as critical may be the cause of potential non-conformities.

6.2 Resourcing

The review of information security controls requires objective analysis and professional reporting skills. Where associated with technical compliance checking, additional specialist skills including a detailed technical knowledge of how security policies have been implemented in software, hardware, over communications links and in associated technical processes are required. Information security control review auditors should have:

- an appreciation of information systems risks and security architectures, based on an understanding of the conceptual frameworks underpinning information systems,
- knowledge of good information security practices such as the information security controls promoted by ISO/IEC 27002 and by other security standards,
- the ability to examine often complex technical information in sufficient depth to identify any significant risks and improvement opportunities, and
- pragmatism with an appreciation of the practical constraints of both information security and information technology reviews.

It is strongly recommended that anyone tasked to conduct an information security controls review, who does not have prior audit experience, be formally acquainted with the fundamentals of audit professionalism: ethics, independence, objectivity, confidentiality, responsibility, discretion, source of authority for access to records, functions, property, personnel, information, with consequent duty of care in handling and safeguarding what is obtained, elements of findings and recommendations, and the follow-up process.

To achieve the review objective, a review team may be created consisting of information security control review auditors with various relevant specialist competencies. Where such skills or competence is not immediately available, the risks and benefits in engaging subject matter experts should be considered, either in the form of in-house, or external, resources to perform the review within the required scope.

Information security control review auditors should also verify that the organization and staff responsible for information security are present, sufficiently knowledgeable in information security and their specific missions, and that they have the necessary resources at their disposal.

As part of an organization's anti-fraud program, information security control review auditors may need to work in close collaboration with financial auditors at each of the audit planning, audit execution and audit review phases.

7 Review methods

7.1 Overview

The basic concept of reviewing controls typically include review procedures, review reporting and review follow-up. The format and content of review procedures include review objectives and review methods.

Information security control review auditors can use three review methods during information security control reviews:

- examine,
- interview, and
- test.

The respective sections include a set of attributes and attribute values for each of the review methods. For the depth attribute, the focused attribute value includes and builds upon the review rigor and level of detail defined for the generalized attribute value. The detailed attribute value includes and builds upon the review rigor and level of detail defined for the focused attribute value. For the coverage attribute, the specific attribute value includes and builds upon the number and type of review objects defined for the representative attribute value. The comprehensive attribute value includes and builds upon the number and type of review objects defined for the specific attribute value.

The “Examine” and “Test” methods can be supported by the use of widely recognized automated tools. Information security control review auditors should also review the impact of the operation of this tool on

normal operation on the review object. When a part of the review relies on such a tool, the information security control review auditor should demonstrate or provide evidence that the tool provides reliable results.

7.2 Review method: Examine

7.2.1 General

The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more review objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of control existence, functionality, correctness, completeness, and potential for improvement over time.

Review objects typically include:

- specifications (e.g., policies, plans, procedures, system requirements, designs),
- mechanisms (e.g., functionality implemented in hardware, software, firmware), and
- processes (e.g., system operations, administration, management, exercises).

Typical information security control review auditor actions may include:

- reviewing information security policies, plans, and procedures,
- analyzing system design documentation and interface specifications,
- observing system backup operations and reviewing the results of contingency plan exercises,
- observing incident response process,
- studying technical manuals and user/administrator guides,
- checking, studying, or observing the operation of an information technology mechanism in the information system hardware/software,
- checking, studying and observing the change management and logging activities relating to an information system, and
- checking, studying, or observing physical security measures related to the operation of an information system.

7.2.2 Attributes

7.2.2.1 Generalized examination

Examinations that typically consist of high-level reviews, checks, observations, or inspections of the review object. This type of examination is conducted using a limited body of evidence or documentation (e.g., functional-level descriptions for mechanisms; high-level process descriptions for processes; and actual documents for specifications). Generalized examinations provide a level of understanding of the control necessary for determining whether the control is implemented and free of obvious errors.

7.2.2.2 Focused examination

Examinations that typically consist of high-level reviews, checks, observations, or inspections and more in depth studies/analyses of the review object. This type of examination is conducted using a substantial body of evidence or documentation (e.g., functional-level descriptions and where appropriate and available, high-level design information for mechanisms; high-level process descriptions and implementation procedures for processes; and the actual documents and related documents for specifications). Focused examinations provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors. They also provide increased grounds for confidence that the control is implemented correctly and operating as intended.

7.2.2.3 Detailed examination

Examinations that typically consist of high-level reviews, checks, observations, or inspections and more in depth, detailed, and thorough studies/analyses of the review object. This type of examination is conducted using an extensive body of evidence or documentation (e.g., functional-level descriptions and where appropriate and available, high-level design information, low-level design information, and implementation information for mechanisms; high-level process descriptions and detailed implementation procedures for processes; and the actual documents and related documents for specifications). Detailed examinations

provide a level of understanding of the control necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

7.2.2.4 Representative examination

Examination that uses a representative sample of review objects (by type and number within type) to provide a level of coverage necessary for determining whether the control is implemented and free of obvious errors.

7.2.2.5 Specific examination

Examination that uses a representative sample of review objects (by type and number within type) and other specific review objects deemed particularly important to achieving the review objective. It also provide a level of coverage necessary for determining whether the control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.

7.2.2.6 Comprehensive examination

Examination that uses a sufficiently large sample of review objects (by type and number within type) and other specific review objects deemed particularly important to achieving the review objective to provide a level of coverage necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

7.3 Review method: Interview

7.3.1 General

The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

Review objects typically include individuals or groups of individuals.

Typical information security control review auditor actions may include interviewing:

- management,
- information asset and mission owners,
- information security officers,
- information security managers,
- personnel officers,
- human resource managers,
- facilities managers,
- training officers,
- information system operators,
- network and system administrators,
- site managers,
- physical security officers, and
- users.

7.3.2 Attributes

7.3.2.1 Generalized interview

Interviews, that consists of broad-based, high-level discussions, with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions. Generalized interviews provide