TECHNICAL SPECIFICATION

ISO/IEC TS 27008

First edition
2019-01

Information technology — Security techniques — Guidelines for the assessment of 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 TS 27008:2019(E)

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

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

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

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

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

This first edition of ISO/IEC TS 27008 cancels and replaces ISO/IEC TR 27008:2011.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document supports the Information Security Risk Management process pointed out in ISO/IEC 27001, and any relevant control sets identified

Information security controls should be fit-for-purpose (meaning appropriate and suitable to the task at hand i.e. capable of mitigating information risks), effective (e.g. properly specified, designed, implemented, used, managed and maintained) and efficient (delivering net value to the organization). This document explains how to assess an organization's information security controls against those and other objectives in order either to confirm that they are indeed fit-for-purpose, effective and efficient (providing assurance), or to identify the need for changes (improvement opportunities). The ultimate aim is that the information security controls, as a whole, adequately mitigate information risks that the organization finds unacceptable and unavoidable, in a reasonably cost-effective and business-aligned manner. It offers the flexibility needed to customize the necessary reviews based on business missions and goals, organizational policies and requirements, known emerging threats and vulnerabilities, operational considerations, information system and platform dependencies, and the risk appetite of the organization.

Please refer to ISO/IEC 27007 for guidelines for information security management systems auditing and ISO/IEC 27006 for requirements for bodies providing audit and certification of information security management systems.

Information technology — Security techniques — Guidelines for the assessment of information security controls

1 Scope

This document provides guidance on reviewing and assessing the implementation and operation of information security controls, including the technical assessment of information system controls, in compliance with an organization's established information security requirements including technical compliance against assessment criteria based on the information security requirements established by the organization.

This document offers guidance on how to review and assess information security controls being managed through an Information Security Management System specified by ISO/IEC 27001.

It 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.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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*

ISO/IEC 27017:2015, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Structure of this document

This document contains a description of the information security control assessment process including technical assessment.

Clause 5 provides background information.

Clause 6 provides an overview of information security control assessments.

Clause 7 presents review methods.

Clause 8 presents the control assessment process.

Annex A supports initial information gathering.

Annex B supports technical assessment.

Annex C supports technical assessment for cloud services.

5 Background

Information security controls are the primary means of treating unacceptable information risks, bringing them within the organization's risk tolerance level.

Parts of an organization's information security controls are usually realized by the implementation of technical information security controls.

An organization's technical security controls can 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 can negatively affect the effectiveness of information security controls and ultimately the quality of the organization's information security standards. Technical assessment is included in ISO/IEC 27002, as one of the controls. A technical assessment is generally performed either manually and/or with the assistance of automated tools. A technical assessment 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.

The output of technical assessment accounts 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 assessment reporting chain should be clearly established at the outset of the assessment and the integrity of the reporting process should be assured. Steps should be taken to ensure that:

— from the outset determine and ensure the appropriate competence in those performing the test(s) — see 6.2,

— relevant accountable parties receive, directly from the information security auditors, an unaltered copy of the technical assessment report;

— inappropriate or unauthorized parties do not receive a copy of the technical assessment report from the information security auditors; and

— the information security auditors are permitted to carry out their work without hindrance/ interference violating the segregation of duty principle.

Information security control assessments, and technical assessments in particular, can 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 the identified information security risk mitigation activities;

— confirm that previously identified or emergent information security vulnerabilities and threats 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.

6 Overview of information security control assessments

6.1 Assessment process

6.1.1 General

For assessments the assigned information security 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). Elements of the assessment work can be prioritized according to the perceived risks but also planned to follow a particular business process or system, or simply designed to cover all areas of the assessment scope in sequence.

When an individual information security control assessment commences, the information security 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 risk assessment to develop assessment documentation to guide the actual assessment work. Supporting information can be found in Annexes A to C.

6.1.2 Preliminary information

Preliminary information can come from a variety of sources:

— books, Internet searches, technical manuals, technical security standards and policies of the organization, and other general background research into common risks and controls in this area, conferences, workshops, seminars or forums;

— results of prior assessments, tests, and audits, whether partially or fully aligned with the present assessment scope and whether or not conducted by information security 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 assessment checklists and articles by information security auditors or information security professionals with expertise in the area related to the scope of the assessment.

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

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

6.1.3 Assessment checklists

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

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

— it lays out the planned areas of assessment work, possibly to the level of detailing individual assessment tests leading to 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 auditors for the assessment fieldwork that follows. Completing the checklist as the assessment progresses, starts the analytical process from which the assessment report will be derived;

— it provides the framework to record the results of assessment pre-work and fieldwork and, for example, a place to reference and comment on assessment evidence gathered;

— it can be reviewed by audit management or other information security auditors as part of the assessment 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 can be required to substantiate or support the review report, inform management and/or help with planning future reviews.

Information security auditors should be cautious 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.

6.1.4 Review fieldwork

The bulk of review fieldwork consists of a series of tests conducted by the information security auditors, or at their requests, to gather review evidence and to review it. It is often done by comparison to anticipated or expected results 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 can check whether all applicable computing platforms have suitable antivirus software. Such review tests often use sampling techniques since there are rarely sufficient review resources to test exhaustively. Sampling practices vary between information security auditors and situations. They 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 assessment sampling approach should be guided, at least in part, by the risks attached to the area of operations being assessed.

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 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 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 interviews with relevant parties and gathered sufficient review evidence, the information security 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.

The evidence should be dispassionately reviewed to check that:

— there is sufficient review evidence to provide a factual basis supporting all of the review findings;

— all findings and recommendations are relevant with regards to the review scope and non-essential matters are excluded; and

— the evidence is appropriately recent and valid with regards the system and controls in scope.

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

6.1.5 The analysis process

As with review planning, the analysis process is essentially risk-based, although it is 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 can choose to accept certain risks identified by information security reviews. In others, they can 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 auditors perform an advisory, non-operational role, but they have significant influence and are backed by sound review practices and factual evidence.

Information security auditors should provide the organization subject to review with reasonable assurance that the information security activities (not all organizations 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 can be considered to ensure this. Information security 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 can be the cause of potential non-conformities.

6.2 Resourcing and competence

The review of information security controls requires objective analysis and professional reporting skills. Where associated with technical assessment, additional specialist skills are required, which include detailed technical knowledge of how security policies have been implemented in software, hardware, over communications links and in associated technical processes. Information security 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 other security standards, including sector-specific security standards where applicable;

— the ability to examine often complex technical information in sufficient depth to identify any significant risks and improvement opportunities;

— pragmatism with an appreciation of the practical constraints of both information security and information technology reviews;

— broad and deep knowledge of security testing tools, operating systems, system administration, communication protocols as well as application security and testing techniques;

— the ability to examine physical security requirements;

— the ability to understand social engineering security requirements.

It is recommended that:

— anyone tasked to conduct an information security control assessment, be familiar with the fundamentals of audit professionalism based on ISO 19011: 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;

— anyone tasked to lead an information security control assessment have enough experience, like at least three years' verified experience, conducting technical information security assessments.

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

Information security 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

— have the necessary resources at their disposal, e.g. time.

7 Review methods

7.1 Overview

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

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

— process analysis;

— examination;

— testing and validation techniques;

— sampling techniques.

Subclauses 7.2 to 7.5 include further considerations for each of the review methods.

Testing and validation can involve automated tools that can be resource-intensive. The potential impact of such tools on operations should be considered when planning their use, for instance scheduling reviews for off-peak times. When a part of the review relies on such a tool, the information security auditor should demonstrate, or provide evidence, that the tool provides reliable results, which establishes the integrity of the tool.

Test and Validate should be mandatory for the following controls if they are marked as "partially operational" or "fully operational".

— B.2.5: ISO/IEC 27002:2013, 9.1 Business requirements of access control

— B.2.5: ISO/IEC 27002:2013, 9.2 User access management

— B.2.5: ISO/IEC 27002:2013, 9.3 User responsibilities

— B.2.5: ISO/IEC 27002:2013, 9.4 System and application access control

— B.2.6: ISO/IEC 27002:2013, 10.1.1 Policy on the use of cryptographic controls

— B.2.8: ISO/IEC 27002:2013, 12.4.2 Protection of log information

— B.2.9: ISO/IEC 27002:2013, 13.1 Network security management

— B.2.10: ISO/IEC 27002:2013, 14.1.2 Securing application services on public networks

— B.2.10: ISO/IEC 27002:2013, 14.1.3 Protecting application services transactions

Review methods may be combined as appropriate depending on the nature of the review and the level of assurance required. Depth of investigation defined with this approach can be:

LOW-DEPTH ASSESSMENT

— Process analysis

MEDIUM-DEPTH ASSESSMENT

— Process analysis

— Examination OR tests on representative sample

IN-DEPTH ASSESSMENT

— Process analysis

— Examination AND tests on extended or exhaustive samples

7.2 Process analysis

7.2.1 General

Directly assessing information security controls such as examination and testing is not always possible or sufficient to be assured of their effectiveness and suitability in operation. It can be more appropriate, or necessary, to deduce the effectiveness and suitability of the controls by analysing the associated processes or activities for evidence confirming that they are:

— designed to provide the desired control effects in theory;

— correctly implemented;

— operating as designed;

— being administered, monitored and managed correctly; and

— actually providing the intended control effects in practice.

The operational and administrative processes or activities are the context within which controls operate, and normally provide evidence of their operation in the form of records, log entries, etc. In particular, the generation and processing of records such as alerts, alarms, events and incident reports by controls generally indicates that they are functional, but can be insufficient to confirm that they are reliable and fully effective. Analysis of the associated processes and activities (e.g. checking procedures, observing and/or interviewing the people involved) in practice provides additional assurance, along with tests to confirm it, that data, criteria or situations, which are expected to trigger the controls, in fact do so.

ISO 19011:2018, B.2 specifies guidelines on how to conduct document reviews.

ISO 19011:2018, B.7 specifies guidelines on how to conduct interviews.

7.3 Examination techniques

7.3.1 General

Examination techniques are a form of review method that facilitates understanding, achieves clarification, or obtains evidence through checks, inspections, reviews, observations, studies, or

analysis of one or more review objects. The purpose of this review is to support the determination of a controls existence, functionality, correctness, completeness, and potential for improvement over time.

Review objects generally include:

— mechanisms (e.g. functionality implemented in hardware, software, firmware, application, database); and

— processes (e.g. system operations, administration, management, exercises).

Typical information security auditor actions can include:

— observing system backup operations and reviewing the results of contingency plan exercises;

— observing incident response process,

— 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;

— checking, studying, or observing physical security measures related to the operation of an information system (e.g. observing secure transport and destruction of disposed confidential paper records);

— reviewing, studying, or observing the configuration of an information system.

7.3.2 Procedural controls

The observation of all kinds of processes without minimally interacting with them (or while doing so) can allow the auditor to receive immediate evidence on how specific activities are performed. The acquisition of related documented information can be used to complete the situation when rare or specific events need to be observed.

7.3.3 Technical controls

Interacting with the review object (directly or via a qualified operator) can allow the auditor to extract or directly review its configuration settings, predicting its behaviour without actually having to test it. This is desirable to deal with critical review objects which can be disturbed by testing techniques or with which the auditor does not have the opportunity to interact.

7.4 Testing an validation techniques

7.4.1 General

Testing and validation techniques are a form of review method that exercises one or more review objects under specified conditions to compare actual with expected behaviour. The results are used to support the determination of control existence, effectiveness, functionality, correctness, completeness, and potential for improvement over time.

Testing has to be executed with great care by competent experts. Possible effects on the operation of the organization have to be considered and approved by management before commencing the testing, and also considering the options of running tests outside maintenance windows, in low charge conditions or even in well reproduced test environments. Failures or unavailability of systems due to testing can have significant impact on the normal business operations of the organization. This can both lead to financial consequences and impact the reputation of the organization. Therefore, particular care has to be taken for the test planning and its correct contractualization (including consideration of legal aspects).

