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).

False positive and false negative results of the tests have to be carefully investigated by the information security auditor before drawing any conclusion.

Typical review objects include mechanisms (e.g. hardware, software, firmware) and processes (e.g. system operations, administration, management; exercises).

Typical information security auditor actions can include:

— testing access control, identification, authentication and review mechanisms;

— testing security configuration settings;

— testing physical access control device;

— conducting penetration testing of key information system components;

— testing information system backup operations;

— testing incident response capability;

— exercising contingency planning capability;

— testing the response of security systems capable of detecting, alerting and responding to intrusions;

— testing encryption and hashing mechanism algorithms;

— testing user id and privilege management mechanisms;

— testing authorization mechanisms;

— verifying the cascade resilience of security measures;

— validating the monitoring and logging;

— validating the security aspects in application development or acquisition of applications.

7.4.2 Blind testing

The information security auditor approaches the review object with no prior knowledge of its characteristics other than publicly available information. The review object is prepared for the review, knowing in advance all the details of the review. A blind review primarily tests the skills of the information security auditor. The breadth and depth of a blind review can only be as vast as the information security auditor's applicable knowledge and efficiency allows. Thus, this testing is of limited use in security reviews and should be avoided.

7.4.3 Double Blind Testing

The information security auditor approaches the review object with no prior knowledge of its characteristics other than publicly available information. The review object is not notified in advance of the scope of the review or the test vectors being used. A double blind review tests the preparedness of the review object to unknown variables.

7.4.4 Grey Box Testing

The information security auditor approaches the review object with limited knowledge of its defences and assets but full knowledge of the test vectors available. The review object is prepared for the review, knowing in advance all the details of the review. A grey box review tests the skills of the information security auditor. The nature of the test is efficiency. The breadth and depth depends on the quality of the information provided to the information security auditor before the test as well as the information security auditor's applicable knowledge. Thus, this testing is of limited use in security reviews and should be avoided. This type of test, often referred to as a Vulnerability Test, is most often initiated by the target as a self-assessment activity.

7.4.5 Double Grey Box Testing

The information security auditor approaches the review object with limited knowledge of its defences and assets but full knowledge of the test vectors available. The review object is notified in advance of the scope and time frame of the review but not the test vectors. A double grey box review tests the target's preparedness to unknown variables. The breadth and depth depends on the quality of the information provided to the information security auditor and the review object before the test as well as the information security auditor's applicable knowledge.

7.4.6 Tandem Testing

The information security auditor and the review object are prepared for the review, both knowing in advance all the details of the review. A tandem review tests the protection and controls of the target. However, it cannot test the preparedness of the target to unknown variables.

The true nature of the test is thoroughness as the information security auditor has a full view of all the tests and their responses. The breadth and depth depends on the quality of the information provided to the information security auditor before the test, as well as the information security auditor's applicable knowledge. This is often known as an In-House Review and the information security auditor often has an active part in the overall security process.

7.4.7 Reversal

The information security auditor approaches the review object with full knowledge of its processes and operational security, but the review object knows nothing of what, how, or when the information security auditor will be testing. The true nature of this test is to review the preparedness of the target to unknown variables and vectors of agitation. The breadth and depth depends on the quality of the information provided to the information security auditor and the information security auditor's applicable knowledge and creativity. This is often called a Red Team exercise.

7.5 Sampling techniques

7.5.1 General

ISO 19011:2018, B.3 specifies guidelines on how to perform sampling.

7.5.2 Representative sampling

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.

7.5.3 Exhaustive sampling

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.

8 Control assessment process

8.1 Preparations

Establishing and retaining an appropriate set of expectations before, during, and after the review is paramount to achieving an acceptable outcome. That means providing information enabling

management to make sound, risk-based, decisions about how to best implement and operate information systems. Thorough preparation by the organization and the information security auditors is an important aspect of conducting effective reviews. Preparatory activities should address a range of issues relating to the cost, schedule, availability of expertise, and performance of the review.

From the organizational perspective, preparing for a review includes the following key activities:

— ensuring that appropriate policies covering reviews are in place and understood by all organizational elements;

— ensuring that all planned steps implementing the controls prior to the review, have been successfully completed and received appropriate management review (this applies only if the control is marked as “fully operational” and not in or while the preparatory/implementation stage);

— ensuring that controls have been assigned to appropriate organizational entities for development and implementation;

— establishing the objective and scope of the review (i.e. the purpose of the review and what is to be reviewed);

— notifying key organizational officials of the impending review and allocating necessary resources to carry out the review;

— establishing appropriate communication channels among organizational officials who are part of the scope in the review;

— establishing time frames for completing the review and key milestone decision points required by the organization to effectively manage the review;

— identifying and selecting a competent information security auditor or audit team that will be responsible for conducting the review, considering issues of information security auditor independence;

— collecting artefacts to provide to the information security auditors (e.g. information security controls documentation including organizational charts, policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements, asset inventories, previous review results);

— establishing a mechanism between the organization and the information security auditors to minimize ambiguities or misunderstandings about control implementation or control weaknesses/ deficiencies identified during the review;

— minimize ambiguities through a mechanism between the organization and the information security auditors, which can take the form of a follow up/tracker document;

— showing the documents presented (by the organization) or requested (by the auditors), and the validity of the documents received in a tracker document. There can be requests for additional information and it is possible to time track unreasonable delay in the provision process.

In addition to the planning activities that the organization carries out in preparation for the review, information security auditors should prepare for the review by:

— understanding the general organization's operations (including mission, functions, and business processes) and how the information assets that are in scope of the review support those organizational operations;

— understanding the general structure of the information assets (i.e. system architecture);

— thoroughly understanding all the controls being reviewed;

— studying relevant publications that are referenced in those controls;

— identifying the organizational entities responsible for the development and implementation of the controls under review that support information security;

— establishing appropriate organizational points of contact needed to carry out the review;

— obtaining artefacts needed for the review (e.g. information security controls documentation including organizational charts, policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements, asset inventories);

— obtaining previous review results that can be appropriately reused for the review (e.g. reports, reviews, vulnerability scans, physical security inspections; developmental testing and evaluation);

— meeting with appropriate organizational officials to ensure common understanding for review objectives and the proposed rigor and scope of the review; and

— developing a review plan.

In preparation for the review of information security controls, the necessary background information should be assembled and made available to the information security auditors. To the extent necessary to support the specific review, the organization should identify and arrange access to elements of the organization (individuals or groups) responsible for developing, documenting, disseminating, reviewing, operating, maintaining and updating all security controls, security policies and associated procedures for implementing policy-compliant controls.

The availability of essential documentation as well as access to key organizational personnel and the information system being reviewed are paramount to a successful review of the information security controls.

8.2 Planning the assessment

8.2.1 Overview

Information security auditors developing plans to review controls should determine the type of control review (e.g. complete or partial review), and which controls/control enhancements are to be included in the review based on the purpose/scope of the review. Information security auditors should estimate and reduce the risk and, where possible, impact of the review on the normal operation of the organization. They should select the appropriate review procedures for the review based on:

— the controls and control enhancements that are to be included in the review; and

— their associate depth and coverage attributes.

Information security auditors should tailor the selected review procedures for the information system risk level and the organization's actual operating environment. If necessary, they should also develop additional review procedures to address security controls, control enhancements and additional assurance needs that are not covered in this document.

Planning the assessment should be documented in an assessment plan. Planning should consider the context, generating the baseline of expected behaviour within the determined context, a specification of the tests/evaluation and the method of validation of the findings within the context of the evaluation.

The plan should also include the development of a strategy to apply the extended review procedure (if necessary, optimization of review procedures) to reduce duplication of effort and provide cost-effective review solutions. After that, information security auditors should finalize the review plan and obtain the necessary approvals to execute the plan.

8.2.2 Scoping the assessment

The scope defines the organizational and technical boundaries of the assessment. The scope of the assessment should be based on a selection of controls depending, for example, on the continuous monitoring schedule established, items on the plan of action and adequate milestones. Controls with greater volatility should be reviewed more frequently.

The scope of the assessment needs to be determined by the information security auditor in conjunction with management, using the organization's documentation. This documentation should provide an overview of the security requirements of the information assets and describe the controls in place or planned for meeting those requirements. The information security auditor starts with the controls described in the information security documentation and considers the purpose of the review. A review can be a complete review of all information security controls in an organization or a partial review of the controls protecting information assets (e.g. during continuous monitoring where subsets of the controls in the information assets are reviewed on an ongoing basis). For partial reviews, the information assets owner collaborates with organizational officials having an interest in the review to determine which controls are to be reviewed.

8.2.3 Review procedures

A review procedure consists of a set of review objectives, each with an associated set of potential review methods and review objects. The determination statements in a review objective are closely linked to the content of the control (i.e. the control functionality). This ensures traceability of review results back to the fundamental control requirements. The application of a review procedure to a control produces review findings. These review findings are subsequently used to help determine the overall effectiveness of the control. The review objects identify the specific items being reviewed and include specifications, mechanisms, processes, and individuals.

Annex A provides examples of review procedures for technical assessment and control enhancements. The Practice guide in Annex A is designed to compile evidence for determining whether controls are implemented correctly, operate as intended, and produce the desired outcome with regard to meeting the information security requirements of the information asset. For each control and control enhancement to be included in the review, information security auditors develop the corresponding review procedure referring to Annex A. The set of selected review procedures varies from review to review based on the current purpose of the review (e.g. annual control review, continuous monitoring). Annex A provides a work sheet for selecting the appropriate review procedures for the review based on the particular review focus.

Review procedures can be tailored by:

— selecting the review methods and objects needed to make appropriate determinations most effectively and to satisfy review objectives;

— selecting the review method depth and coverage attribute values necessary to meet the review expectations based on the characteristics of the controls being reviewed and the specific determinations to be made;

— eliminating review procedures for controls if they have been reviewed by another adequate review process;

— developing information system/platform-specific and organization-specific review procedure adaptations to carry out the review successfully;

— incorporating review results from previous reviews where the results are deemed applicable;

— making appropriate adjustments in review procedures to be able to obtain the requisite review evidence from suppliers, if present; and

— selecting review methods with due consideration for their organizational impacts while ensuring that audit objectives are met.

8.2.4 Object-related considerations

Organizations can specify, document and configure their information assets in a variety of ways and the content and applicability of existing review evidence will vary. This can result in the need to apply a variety of review methods to various review objects to generate the review evidence needed to determine whether the controls are effective in their application. Therefore, the list of review methods and objects provided with each review procedure is called "potential" to reflect this need to be able to choose the methods and objects most appropriate for a specific review. The review methods and objects chosen are those deemed necessary to produce the review evidence needed. The potential methods and objects in the review procedure are provided as a resource to assist in the selection of appropriate methods and objects, and not with the intent to limit the selection. As such, information security auditors should use their judgment in selecting from the potential review methods and the general list of review objects associated with each selected method.

Information security auditors should select only the methods and objects that contribute most effectively to making the determination process associated with the review, objective. Measure of the quality of the review results is based on the soundness of the rationale provided, not the specific set of methods and objects applied. In most cases, it is not necessary to apply every review method to every review object to obtain the desired review results. For specific or comprehensive reviews, it can be appropriate to use a method not currently listed in the set of potential methods, or not to use a method that is listed.

8.2.5 Previous findings

8.2.5.1 Overview

Information security auditors should take advantage of existing control review information to facilitate more effective reviews. The reuse of review results from previously accepted or approved reviews of the information system should be considered in the body of evidence for determining overall control effectiveness.

When considering the reuse of previous review results and the value of those results to the current review, information security auditor should determine:

— the credibility of the evidence;

— the appropriateness of previous analysis; and

— the applicability of the evidence to current information asset conditions.

It can be necessary, in certain situations, to supplement the previous review results under consideration for reuse with additional review activities to fully address the review objectives. For example, if an independent third-party evaluation of an information technology product did not test a particular configuration setting that is used by the organization in an information system, then it is possible that the information security auditor will need to supplement the original test results with additional testing to cover that configuration setting for the current information system environment.

Subclauses 8.2.5.2 to 8.2.5.4 should be considered in validating previous review results for reuse in current reviews.

8.2.5.2 Changing conditions

Controls that were deemed effective during previous reviews can have become ineffective due to changing conditions relating to the information asset or the surrounding environment. Thus, it is possible that review results that were found to be previously acceptable, no longer provide credible evidence for determination of control effectiveness, and a new review is required. Applying previous review results to a current review requires the identification of any changes that have occurred since the previous review and the impact of these changes on the previous review results. For example, reusing previous review results that involved examining an organization's security policies and

procedures can be acceptable if it is determined that there have not been any significant changes to the identified policies, procedures and risk environment.

8.2.5.3 Acceptability of reusing reviews.

The acceptability of using previous review results in a control review should be coordinated with and approved by the users of the review results. It is essential that the information asset owner collaborate with appropriate organizational officials (e.g. chief information officer, chief information security officer, mission/information owners) in determining the acceptability of using previous review results. The decision to reuse review results should be documented in the review plan and the final report.

Security reviews can include the findings from a previous security review as long as:

— it is expressly permitted in the assessment plan;

— any constraints or issues from a previous review should be documented with their relevance to this review. This includes issues partially resolved by ongoing action plans;

— information security auditors have good grounds to believe the findings remain valid;

— any technology or procedural changes to the controls or the processes to which they are applied are given adequate security consideration in the current review; and

— the use and any potential risk management implications of adopting prior assessment findings are clearly stated in the assessment report.

8.2.5.4 Time aspects

In general, as the time period between current and previous reviews increases, the credibility/utility of the previous review results decreases. This is primarily due to the fact that information assets, or the environment in which the information assets operate, are more likely to change with time, possibly invalidating the original conditions or assumptions on which the previous review was based.

8.2.6 Work assignments

Information security auditor independence can be a critical factor in certain types of reviews, especially for information assets at the moderate and high-risk levels. The degree of independence required from review to review should be consistent. For example, it is not appropriate to reuse results from a previous self-assessment where information security auditor independence was not required, in a current review requiring a greater degree of independence.

8.2.7 External systems

The review methods and procedures in Annex A need to be adjusted as appropriate to accommodate the review of external information systems. Because the organization does not always have direct control over the security controls used in external information systems, or sufficient visibility into the development, implementation, and review of those controls, it can be necessary to apply alternative review approaches. This can result in the need to tailor the review procedures described in Annex A. Where required assurances of agreed-on controls for an information system are documented in contracts or service-level agreements. The information security auditor should review these contracts or agreements and, where appropriate, tailor the review procedures to review either the controls or the control review results provided through these agreements. Additionally, information security auditors should take into account any reviews that have been conducted, or are in the process of being conducted, by organizations operating external information systems that are relied on with regard to protecting the information assets under review. If deemed reliable, applicable information from these reviews should be incorporated into the report.

8.2.8 Information assets and organization

Review procedures can be adapted to address system/platform-specific or organization-specific dependencies. This situation arises frequently in the review procedures associated with the technical information security controls (i.e. access control, audit and accountability, identification and authentication, system and communications protection). Recent test results can also be applicable to the current review if those test methods provide a high degree of transparency (e.g. what was tested, when was it tested, how was it tested). Standards-based testing protocols can provide examples of how organizations can help achieve this level of transparency.

8.2.9 Extended review procedure

Organizations have great flexibility in achieving information security control assurance requirements. For example, for a requirement such as assurance that flaws are addressed in a timely manner, the organization can satisfy this requirement on a control-by-control basis, on a by-type-of-control basis, on a system-by-system basis, or perhaps even at the organizational level. In consideration of this flexibility, the extended review procedure is generally applied on a review-by-review basis according to how the organization chose to achieve assurances for the information asset under review. The method of application should be documented in the review plan. Further, the organization selects the appropriate review objectives from the extended review procedure based on the information asset risk level. The application of the extended review procedure is intended to supplement the other review procedures to increase the grounds for confidence that controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the applicable information security requirements.

8.2.10 Optimization

Information security auditors can have a certain degree of flexibility in organizing a review plan that meets the needs of the organization. This is an opportunity to obtain the necessary evidence in determining security control effectiveness, while reducing overall review costs.

Combining and consolidating review procedures is one area where this flexibility can be applied. During the review, review methods are applied numerous times to a variety of review objects within a particular area of information security controls.

To save time, reduce review costs and maximize the usefulness of review results, information security auditors should review the selected review procedures for the control areas and combine or consolidate the procedures (or parts of procedures) whenever possible or practicable.

For example, information security auditors can wish to consolidate interviews with key organizational officials dealing with a variety of information security-related topics. Information security auditors can have other opportunities for significant consolidations and cost savings by examining all applicable security policies and procedures at the same time or organizing groups of related policies and procedures that can be examined as a unified entity. Obtaining and examining configuration settings from similar hardware and software components within relevant information systems is another example that can provide significant review efficiencies.

An additional area for consideration in optimizing the review process is the sequence in which controls are reviewed. The review of some controls before others can provide information that facilitates understanding and review of other controls. For example, control areas can produce general descriptions of the information assets. Reviewing these security controls early in the review process can provide a basic understanding of the information assets that can aid in reviewing other security controls. The supplemental guidance of many controls also identifies related controls that can provide useful information in organizing the review procedures. In other words, the sequence in which reviews are conducted can facilitate the reuse of review information from one control in reviewing other related controls.

8.2.11 Finalization

After selecting the review procedures (including developing necessary procedures not contained in this document), tailoring the procedures for information asset-specific and organization-specific conditions, optimizing the procedures for efficiency, applying the extended review procedure where necessary, and addressing the potential for unexpected events impacting the review, the review plan is finalized and the schedule is established including key milestones for the review process.

Once the review plan is completed, the plan is reviewed and approved by appropriate organizational officials to ensure that the plan is:

— complete;

— consistent with the security objectives of the organization and the organization's review of risk; and

— cost-effective with regard to the resources allocated for the review.

In case the review can interrupt the normal operation of the organization [e.g. by blocking key personal or possible (temporary) failures of systems due to penetration testing], the review plan needs to highlight the extent and timeframe of these interruptions.

8.3 Conduction reviews

After the review plan is approved by the organization, the information security auditor executes the plan in accordance with the agreed milestones and schedule.

Review objectives are achieved by applying the designated review methods to selected review objects and compiling/producing the information necessary to make the determination associated with each review objective. Each determination statement contained within a review procedure carried out by an information security auditor can have one of the following findings:

— Satisfied (S);

— Partly satisfied (P); or

— Not satisfied (O).

"Satisfied" means that, for the portion of the control addressed by the determination statement, the review information obtained (i.e. evidence collected) indicates that the review objective for the control has been met producing a fully acceptable result.

"Partly satisfied" means that a portion of the control is not addressing its objective or that, at the time of the review, the implementation of the control is still in progress, with reasonable assurance that the control will reach a satisfied result (S).

"Not satisfied" means that, for the portion of the security control addressed by the determination statement, the review information obtained indicates potential anomalies in the operation or implementation of the control that need to be addressed by the organization. If the finding is "not satisfied", it can also indicate that, for reasons specified in the review report, the information security auditor was not able to obtain sufficient information to make the particular determination requested in the determination statement.

The information security auditor findings (i.e. the determinations made) should be an unbiased, factual reporting of what was found concerning the control reviewed. For each "not satisfied", information security auditors should indicate which parts of the security control are affected (i.e. the aspects of the control that were deemed not satisfied or were not able to be reviewed) and describe how the control differs from the planned or expected state. The information security auditor should also note the potential for compromises to confidentiality, integrity, and availability due to findings "not satisfied". If the review reveals major non-conformities (i.e. findings "not satisfied" which deviate significantly from the planned status), which can create a significantly increased risk for the organization, the information

security auditor should immediately inform the person responsible for this control and management so that mitigation procedures can be initiated immediately.

8.4 Analysis and reporting results

The review plan provides the objectives for the review and a detailed roadmap of how to conduct such a review. The output and end result of the review is the review report, which documents the information assurance level based on the implemented information security controls. The report includes information from the information security auditor (in the form of review findings) necessary to determine the effectiveness of the controls employed and the organization's overall effectiveness in implementing appropriate controls based on the information security auditor's findings. The report is an important factor in determining the information security risks to operations (i.e. mission, functions), organizational assets, individuals and other organizations.

Review results should be documented at the level of detail appropriate for the review in accordance with a reporting format prescribed by organizational policy. The reporting format should also be appropriate for the type of control review conducted (e.g. self-assessment by information system owners, independent verification and validation, independent control reviews by auditors).

The information system owner relies on the information security expertise and the technical judgment of the information security auditor to review the security controls and provide specific recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities.

The review information produced by the information security auditor (i.e. findings "satisfied" or "not satisfied", identification of the parts of the security control that did not produce a satisfactory result, and a description of resulting potential for compromises to the information asset) is provided to managers in the initial (draft) security review report. Asset owners can choose to:

— act on selected information security auditor recommendations before the report is finalized if there are specific opportunities to correct weaknesses or deficiencies in the controls;

— or to correct/clarify misunderstandings or interpretations of review results.

The information security auditor should review again the controls which are modified, enhanced or added during this process before producing the final report. The delivery of the final report to management marks the official end of the information security control review.

Since results of the review ultimately influence the content of information security controls and the plan of action and milestones, the information asset owner reviews the findings of the information security auditor and, with the concurrence of management, determines the appropriate steps required to correct weaknesses and deficiencies identified during the review. By using the tags satisfied (S), partly satisfied (P) and other than satisfied (O), the reporting format for the review findings provides visibility for managers into specific weaknesses and information security deficiencies, and facilitates a disciplined and structured approach to mitigating risks in accordance with the information security risk management process.

For example, the information asset owner in consultation with managers can decide that certain review findings marked as not satisfied are of an inconsequential nature and present no significant risk to the organization. Alternatively, the asset owner and managers can decide that certain findings marked as not satisfied are significant, requiring immediate remediation actions. In all cases, the organization reviews each information security auditor finding of not satisfied and applies its judgment with regard to the severity or seriousness of the finding (i.e. the potential adverse effect on the organization's operations and assets, individuals, other organizations, etc.), and whether the finding is significant enough to justify further investigation or remedial action. Senior management involvement in the mitigation process can be necessary in order to ensure that the organization's resources are effectively allocated in accordance with organizational priorities. This can be by providing resources firstly to the information assets that are supporting the organization's most business-critical processes, or by correcting the deficiencies that pose the greatest degree of risk. Ultimately, the review findings and any subsequent mitigation actions initiated by the information asset owner in collaboration with designated

organizational officials trigger updates to the information security risk management process and information security controls. Therefore, the key documents used by the managers to determine the information security status of the information assets are updated to reflect the results of the review.

At pre-determined milestones or fixed periods after the review, e.g. three months after final reporting, a follow-up review focusing on the outstanding or open issues is performed. This includes verifying the validity of implemented solutions to previous findings. Organizations can also choose to conduct follow-up activities at the next review, especially for the issues that are non-critical or urgent.

Annex A
(Informative)

Initial information gathering (other than IT)

A.1 General

A.1.1 Human resources and security

a) Does the personnel feel responsible and/or accountable for his/her actions?

b) Is there security and information security knowledge available on-site to answer questions, motivate the personnel and provide the needed guidance?

c) Are applicable policies and procedures clear and SMART (specific, measurable, acceptable, realistic and time-related)?

d) Is personnel hired in accordance with the expected operational knowledge?

e) Are the personnel trustable to handle sensitive information and systems that would endanger the survival of the organization?

f) Are the personnel effectively trusted?

g) How is this trust defined and measured?

h) Are background checks performed?

A.1.2 Policies

a) Strategic alignment:

   1) Are the information security policies derived from the business objectives and from the overall security policy?

   2) How the link is made with the IT, HR, acquisition policies, etc.?

b) Comprehensive:

   1) Are the policies addressing information security in all business activity sectors (HR, physical, IT, sales, production, R&D, contacts, etc.)?

   2) Are the policies complete in their design encompassing strategy, tactics, and operations?

c) Formulation:

   1) Are the policies a “copy-paste” of ISO/IEC 27002, or are the control objectives and controls tailored to the specific context?

   2) Are the policies written to clearly identify the responsible actor(s)?

   3) An action expected within a policy or a procedure should consider the fundamental questions: who, when, why, what, where, how.

      i) If the person responsible (who) to perform the action is not defined, who will achieve the set objectives?

ii) If the target time (when) for performing the action is not defined, will it be started or finished in due time?

iii) If the aim or objective of an action is not defined (why), will the action be correctly understood and its importance adequately considered?

iv) If the action itself (what) is not defined, how will it be possible to perform it?

v) If an action doesn't define the object, place, process, information asset or "control" on which it has to have an effect, how will it be effective (where)?

vi) If an action in a procedure doesn't clearly define how things have to be done, how can it correctly performed (how)?

vii) If an action doesn't also define the indicators and controls aimed at verifying it correctly evolves and achieves its objectives, how can an organization make sure the objectives are, or can be, achieved?

4) Are there controls and a checking environment in place to identify if the policy statements are enforced implemented and the goals achieved?

5) The objectives in a policy statement should consider the SMART criteria. If not:

i) unspecific objectives are not easy to clearly recognize and the person(s) responsible to achieve it is generally not defined;

ii) if the objective is not measurable, there is little chance that an organization will be able to verify if it is achieved or not;

iii) if the objective is not communicated and acceptable to the personnel who have to cope with, there is great chance the control will be misunderstood, circumvented or "disconnected";

iv) if the objective is not realistic, in relation to the real capability of the organization, there is little chance it will ever be achieved; and

v) if the objective is not defined in relation with time (when it has to be achieved, when the action is supposed to start, etc.) there is a good chance that no action will be taken and the objective never met.

A.1.3 Organization

a) Is the set of roles and responsibilities defined and allocated, which are necessary and sufficient to meet business objectives taking into account the specific context and constraints?

b) Is the link with external authorities defined?

c) Are security responsibilities outsourced if the organization has no internal capability?

d) Is information security addressed in contracts?

A.2 Physical and environmental security

A.2.1 Are the sites safe for information?

a) Zones

1) Are areas accessible to the public sufficiently isolated from business areas?

2) Are there zones defined where more critical information is handled (by people or ICT system)?

3) Are these secured zones appropriately segregated to avoid information exchange?

b) Locations

1) Are the different zones clearly identified and appropriately situated?

2) Are the borders (walls, ceiling, floor, etc.) clearly defined and their solidity appropriate for the protection of the contained assets?

3) Are the locations appropriately labelled and the critical ones out of sight of external people?

c) Gates — access points

1) Do doors, windows and openings in the borders provide the same protection as the borders when they are closed?

2) Is an appropriate access control in place to enter and exit the zone?

3) Is there an anti-intrusion system?

4) Are there emergency exits allowing for enough mobility of information, people and equipment?

d) Corridors and paths

1) Are paths to the zones and locations identified:

i) Paths for people;

ii) Cables (paths for information).

2) Are there alternative paths?

3) Are these paths protected and monitored?

e) Monitoring

1) Can the monitoring resources see without being seen?

2) Can the monitoring resources see an intrusion coming from a distance?

3) When is monitoring active?

4) Where and how are records kept and analysed?

f) Furniture

1) Appropriate for information storage?

2) Correctly located?

3) Operating as expected?

A.2.2 Are the sites safe for ICT? (Environmental aspects)

a) Power provision

1) Enough/Appropriate

2) Alternate?

b) Air conditioning provision

1) Enough/Appropriate

2) Alternate?

c) Fire-fighting provision

1) Enough/Appropriate

2) Alternate?

A.2.3 Are the sites safe for people?

a) Do emergency exits exist (and with appropriate controls)?

b) Is leakage (power supply, water, gas, liquids) a potential danger for people?

c) Are temperature, humidity, stuff and vibrations a potential danger for people?

d) Is equipment located so that people cannot be injured?

e) Are the gates installed and operated so that people cannot be injured?

f) Is furniture installed and maintained so that people cannot be injured?

A.3 Incident management

a) Are information security incidents defined?

b) Is there a capability build to respond to information security incidents?

1) Guidelines?

2) Roles and responsibilities?

Annex B
(informative)

Practice guide for technical security assessments

B.1 General

This annex provides a set of practical guides for technical assessment by using typical technical controls depicted from ISO/IEC 27002. Each control in this annex is basically organized by the following structure of statements and guidance. ISO/IEC 27001 does not require the controls that an organization uses to be selected from ISO/IEC 27002. Other controls, such as the sector-specific controls in standards such as ISO/IEC 27010 and ISO/IEC 27017 can be necessary. Moreover, organizations may design their own controls. However, using examples from ISO/IEC 27002 is enough for the purposes of this annex, since it aims to illustrate various technical assessment techniques that can be used.

Subclauses B.2.1 to B.2.14 present a table for each control from ISO/IEC 27002, whose contents are grouped by the following terms.

"Technical control" (with "additional technical information")

1) Security implementation standard (with "technical note on security implementation standard")

   1.1) Practice guide, Evidence assumed, Method

   1.2) Practice guide, Evidence assumed, Method

2) Security implementation standard (with "technical note on security implementation standard")

   2.1) Practice guide, Evidence assumed, Method

   2.2) Practice guide, Evidence assumed, Method

Each technical control has additional technical information to give further support to information security auditors. It basically consists of a series of "security implementation standards" which should be regularly reviewed by the organization to verify whether applicable standards are appropriately implemented and operated or not.

Each "security implementation standard" has a supplementary "technical note on security implementation standard" to give further technical information for the reviewing process. It also provides a series of "Practice guide", "Evidence assumed" and "Method".

"Practice guide" provides a compliance checking procedure to be applied for the security implementation standard. "Evidence assumed" gives some examples of systems, files, documents or other items, which can be accepted as "evidences" in the compliance checking procedure. Please note that the names of the evidence can differ among organizations. However, the names used in this annex can be considered as generally accepted in the field of technical assessment. "Method" provides an appropriate approach to technical assessment in accordance with the Practice guide above.

This annex does not provide exhaustive Practice guides for technical assessment, but will still greatly help organizations to review whether security implementation standards are appropriately implemented, and operated, or not.

B.2 Assessment of controls from ISO/IEC 27002

B.2.1 ISO/IEC 27002:2013, Clause 5 Information security policies

ISO/IEC 27002:2013, 5.1 Management direction for information security		
	Control	**ISO/IEC 27002:2013, 5.1.1, Policies for information security** A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.
	Control	**ISO/IEC 27002:2013, 5.1.2, Review of the policies for information security** The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

B.2.2 ISO/IEC 27002:2013, Clause 6 Organization of information security

ISO/IEC 27002:2013, 6.1 Internal organization		
	Control	**ISO/IEC 27002:2013, 6.1.1, Information security roles and responsibilities** All information security responsibilities should be defined and allocated.
	Control	**ISO/IEC 27002:2013, 6.1.2, Segregation of duties** Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
	Control	**ISO/IEC 27002:2013, 6.1.3, Contact with authorities** Appropriate contacts with relevant authorities should be maintained.
	Control	**ISO/IEC 27002:2013, 6.1.4, Contact with special interest groups** Appropriate contacts with relevant authorities should be maintained.
	Control	**ISO/IEC 27002:2013, 6.1.5, Information security in project management** Information security should be addressed in project management, regardless of the type of the project.

ISO/IEC 27002:2013, 6.2 Mobile devices and teleworking		
	Control	**ISO/IEC 27002:2013, 6.2.1, Mobile device policy** A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.
	Control	**ISO/IEC 27002:2013, 6.2.2, Teleworking** A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.

B.2.3 ISO/IEC 27002:2013, Clause 7 Human resource security

ISO/IEC 27002:2013, 7.1 Prior to employment		
	Control	**ISO/IEC 27002:2013, 7.1.1 ,Screening** Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
	Control	**ISO/IEC 27002:2013, 7.1.2, Terms and conditions of employment** The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.

ISO/IEC 27002:2013, 7.2 During employment		
	Control	**ISO/IEC 27002:2013, 7.2.1, Management responsibilities** Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
	Control	**ISO/IEC 27002:2013, 7.2.2, Information security awareness, education and training** All employees of the organization and, where relevant, contractors should receive appropriate awareness, education and training and regular updates in organizational policies and procedures, as relevant for their job function.
	Control	**ISO/IEC 27002:2013, 7.2.3, Disciplinary process** There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

ISO/IEC 27002:2013, 7.3 Termination and change of employment		
	Control	**ISO/IEC 27002:2013, 7.3.1, Termination or change of employment responsibilities** Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.

B.2.4 ISO/IEC 27002:2013, Clause 8 Asset management

ISO/IEC 27002:2013, 8.1 Responsibility for assets		
	Control	**ISO/IEC 27002:2013, 8.1.1, Inventory of assets** Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.
	Control	**ISO/IEC 27002:2013, 8.1.2, Ownership of assets** Assets maintained in the inventory should be owned.
	Control	**ISO/IEC 27002:2013, 8.1.3, Acceptable use of assets** Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.
	Control	**ISO/IEC 27002:2013, 8.1.4, Return of assets** All employees and external party users should return all of the organizational assets in their possession on termination of their employment, contract or agreement.

ISO/IEC 27002:2013, 8.2 Information classification		
	Control	**ISO/IEC 27002:2013, 8.2.1, Classification of information** Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
	Control	**ISO/IEC 27002:2013, 8.2.2, Labelling of information** An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.
	Control	**ISO/IEC 27002:2013, 8.2.3, Handling of assets** Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.

ISO/IEC 27002:2013, 8.3 Media handling		
	Control	**ISO/IEC 27002:2013, 8.3.1, Management of removable media** Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
	Control	**ISO/IEC 27002:2013, 8.3.2, Disposal of media** Media should be disposed of securely when no longer required, using formal procedures.
	Control	**ISO/IEC 27002:2013, 8.3.3, Physical media transfer** Media containing information should be protected against unauthorized access, misuse or corruption during transportation.

B.2.5 ISO/IEC 27002:2013, Clause 9 Access control

ISO/IEC 27002:2013, 9.1 Business requirements of access control			
	Control	**ISO/IEC 27002:2013, 9.1.1, Access control policy** An access control policy should be established, documented and reviewed based on business and information security requirements.	
	Additional technical information on the Control	Access control rules should be supported by formal procedures and defined responsibilities. Role based access control is an approach used successfully by many organisations to link access rights with business roles.	
1	Security implementation standard	Access control can be implemented through many different methods including: — PIM (Privileged Identity Management); — electronic locking systems; — porter services; — SIEM (Security Information and Event Management). NOTE Some of these methods have limitation. For instance, SIEM can only analyse and store logs occurring while using some form of access control. Electronic locking systems can be used to control physical access to a resource. And PIM can be used to manage identities and their access rights.	
	Technical note on Security implementation standard	The complexity of access controls increases with the asset it protects, the threat of an attack, and the impact of a successful attack.	
	1.1	Practice guide	Check that only authorized people get access to a resource
		Evidence assumed	— Access logs — Access to an access control mechanism
		Method	Test and Validate
	1.2	Practice guide	Check if access rights will be removed, when they are no longer necessary
		Evidence assumed	— Revoked identity for testing — Access logs — Access to a user administration
		Method	Test and Validate
	1.3	Practice guide	Check if the process of access requests can be bypassed without a privileged account

ISO/IEC 27002:2013, 9.1 Business requirements of access control			
		Evidence assumed	— Access logs — Identity without access rights — Identity with privileges for comparison — Access to an access control mechanism
		Method	Test and Validate
	1.4	Practice guide	Check that all access events get logged and can be analysed for forensic purposes
		Evidence assumed	— Log files — Business requirements for logs
		Method	Test and Validate
	1.5	Practice guide	Check if it is possible escalate privileges to access resources
		Evidence assumed	— Access logs — Identity without access rights — Access to an access control mechanism
		Method	Test and Validate
	1.6	Practice guide	Check that it is not possible to bypass the access controls
		Evidence assumed	— Access logs — Identity without access rights — Access to an access control mechanism
		Method	Test and Validate
	1.7	Practice guide	Check if access rights are black or whitelisted and check that no assets are missing
		Evidence assumed	— Business requirements — Business requirements of access control — Access to access control management interface
		Method	Test and Validate
	1.8	Practice guide	Check that it is not possible to clone or reproduce access tokens or to impersonate someone else
		Evidence assumed	— Identity without access rights — Identity with access rights to be impersonated — Access to an access control mechanism
		Method	Test and Validate
	Control	**ISO/IEC 27002:2013, 9.1.2, Access to networks and network services** Users should only be provided with access to the network and network services that they have been specifically authorized to use.	
	Additional technical information on the Control	Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's information security management and control.	
1	Security implementation standard	A policy should be formulated concerning the use of networks and network services.	

ISO/IEC 27002:2013, 9.1	Business requirements of access control		
	Technical note on Security implementation standard	This policy should cover: a) the networks and network services which are allowed to be accessed; b) authorization procedures for determining who is allowed to access which networks and networked services; c) management controls and procedures to protect access to network connections and network services; d) the means used to access networks and network services (e.g. use of VPN or wireless network); e) user authentication requirements for accessing various network services; f) monitoring use of network services. The policy on the use of network services should be consistent with the organization's access control policy.	
	1.1	Practice guide	Use network sniffing to identify emanating protocols from network service responses or requests where applicable. For example, Netbios, ARP, OSPF, etc.
		Evidence assumed	— Access to network traffic
		Method	Test and Validate
	1.2	Practice guide	Verify broadcast requests and responses from all targets are in line with network diagrams and other documents.
		Evidence assumed	— Access to network diagrams — Access to network traffic
		Method	Test and Validate
	1.3	Practice guide	Discover and identify all open ports and services within the authorized network by running port scans. Request all service banners (flags) for discovered TCP and UDP ports. Verify that the discovered services are justified based on user privileges and system functions.
		Evidence assumed	— Access to system specifications — Port scanning is allowed in the subject network
		Method	Test and Validate
	1.4	Practice guide	Test measures to access services within the network or other networks via address spoofing.
		Evidence assumed	— Address-spoofing can be conducted in a test or non-critical environment
		Method	Test and Validate
	1.5	Practice guide	Enumerate and identify all systems with footholds in other restricted networks via multiple network cards. Attempt to compromise these entry points in order to pivot into restricted networks.
		Evidence assumed	— Complete Network diagrams
		Method	Test and Validate
	1.6	Practice guide	Enumerate and identify all remote desktop services which can be used to gain access to systems outside of the authorized network. Attempt to gain unauthorized access via remote desktop in order to pivot into restricted networks.
		Evidence assumed	— Complete Network diagrams — Remote desktop services available connected to systems outside of the authorized network

ISO/IEC 27002:2013, 9.1 Business requirements of access control			
		Method	Test and Validate
	1.7	Practice guide	Examine and validate firewall rules to ensure only intended access is granted to networks and network services.
		Evidence assumed	— Access to firewall rules — Access to firewall logs
		Method	Test and Validate

ISO/IEC 27002:2013, 9.2 User access management			
	Control	**ISO/IEC 27002:2013, 9.2.1, User registration and de-registration** A formal user registration and de-registration process should be implemented to enable assignment of access rights.	
	Additional technical information on the Control	Formal processes should be utilized to allocate, restrict and control privileged user access to networks, services and resources.	
1	Security implementation standard	The following processes should be documented and implemented: — User registration and de-registration; — User access provisioning; — Management of privileged access rights; — Management of secret authentication information of users; — Review of user access rights; — Removal or adjustment of access rights.	
	Technical note on Security implementation standard	The allocation of privileged access rights should be controlled through a formal authorization process in accordance with the relevant access control policy	
	1.1	Practice guide	Verify that all user ID's are unique and person-specific. Validate through spot checks that former employee accounts are no longer active. Verify that there are no user ID's which have not been used for an abnormally long period of time.
		Evidence assumed	— Access to the user management administration — Access to a list of former employees or user ID's
		Method	Test and Validate
	1.2	Practice guide	Ensure that the password complexity makes guessing passwords difficult and that the username is not public information such as email address or social security number.
		Evidence assumed	— Access to the password policy — Username and password-based authorization
		Method	Test and Validate
	1.3	Practice guide	Ensure that the user must respond to a secret answer or secret question or other predetermined information before passwords can be reset.
		Evidence assumed	— Access to the password policy — Username and password-based authorization — Access to a password reset function — Authorized test account
		Method	Test and Validate

ISO/IEC 27002:2013, 9.2 User access management			
	1.4	Practice guide	Ensure that the users account is locked out for a period of time when the incorrect password is entered more than a specific number of times.
		Evidence assumed	— Authorized test account — Username and password-based authorization
		Method	Test and Validate
	1.5	Practice guide	— Enumerate the use of default accounts on targets. Test access to authenticated access points through the most appropriate and available cracking techniques.
		Evidence assumed	— Username and password-based authorization
		Method	Test and Validate
	Control	**ISO/IEC 27002:2013, 9.2.2, User access provisioning** A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	
	Control	**ISO/IEC 27002:2013, 9.2.3, Management of privileged access rights** The allocation and use of privileged access rights should be restricted and controlled.	
	Additional technical information	Privilege management is important, because the inappropriate use of privilege causes significant impact to the systems. The status of allocation of privilege should be described in the documents, which defines privilege (privilege definition document). Because the access privileges associated with each system product (operating system, database management system, and each application) are different. Example of types of privilege are: — Root (UNIX, Linux), — Administrator (Windows), — Backup Operator (Windows), — Power User (Windows), — SA (DBMS), and — DB admin (DBMS). The allocation of privilege should be minimum on a need-to-use basis. Also, it is not necessarily to be allocated constantly. The method of privilege management is different in systems. Example of privilege management based on systems are: — In operating system, ACL (Access Control List) defines privilege, — In DBMS, it defines variety of default privileges, — In application, it may define variety of default privileges for application's management function, so information security auditors should determine level of check in advance, and — In secure OS, it has a function of mandatory access control.	
1	Security implementation standard	The access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated should be identified.	

ISO/IEC 27002:2013, 9.2 User access management			
	Technical note on Security implementation standard	The activity of privilege users should be monitored, because of inappropriate use of privilege causes a significant impact the systems. The methods for detecting inappropriate use of privilege are different if system architecture is different. NOTE Representative system architectures are: — Mainframe, — Windows, — UNIX, Linux, and — Secure OS.	
	1.1	Practice guide	Check that allocation of privilege has been described in privilege definition document.
		Evidence assumed	Privilege definition document
		Method	Examine/Observe
	1.2	Practice guide	Check that setting of system configuration as described in documents which defines privilege. The checking method of privilege's operation is different in system architecture. Examples of checking method of privilege's operation. 1) (In case of Mainframe) Check the status of utilization of privileges is appropriate by checking RACF report. 2) (In case of UNIX, Linux, or Windows) Check that status of utilization of privileges is appropriate by investigating logs, which show use of privilege. NOTE: 1) RACF (Resource access control facility) is a security management middleware in mainframe. 2) In UNIX or Linux, it is dangerous to check only log-on by root to investigate inappropriate use of root. The reason for it is that normal user may become root by using 'su' command after log-on in UNIX or Linux.
		Evidence assumed	— Privilege definition document — Access Control List — RACF report
		Method	Examine/Observe
2	Security implementation standard	Privilege should be assigned to a different user ID from those used for normal business use.	
	Technical note on security implementation standard	In case of access by privilege, it has a possibility of unauthorized operation by contingent, and the situation of using the privilege regularly become hotbeds for unauthorized access. Users should use their regular ID if the operation does not need the privilege. If the login by 'root' privilege is permitted, it is impossible to identify who was login to the system from the log.	
	2.1	Practice guide	Check whether privileged users have normal user ID beside privilege ID by observing the ACLs of the systems.
		Evidence assumed	— Access Control List
		Method	Examine/Observe

ISO/IEC 27002:2013, 9.2 User access management			
	2.2	Practice guide	Check that the privileged user uses a different user ID for normal business by observing log files. In case of UNIX or Linux, check the system configuration promotes that the system denies login by 'root'. NOTE Information security auditors should try interview to check the privileged user uses a different user ID for normal business use when the log indicates that privileged user uses only privilege ID.
		Evidence assumed	— Log file — System configuration of login by 'root'
		Method	Examine/Observe
	Control	**ISO/IEC 27002:2013, 9.2.4, Management of secret authentication information of users** The allocation of secret authentication information should be controlled through a formal management process.	
	Control	**ISO/IEC 27002:2013, 9.2.5, Review of user access rights** Asset owners should review users' access rights at regular intervals.	
	Control	**ISO/IEC 27002:2013, 9.2.6, Removal or adjustment of access rights** The access rights of all employees and external party users to information and information processing facilities should be removed on termination of their employment, contract or agreement, or adjusted on change.	

ISO/IEC 27002:2013, 9.3 User responsibilities		
	Control	**ISO/IEC 27002:2013, 9.3.1, Use of secret authentication information** Users should be required to follow the organization's practices in the use of secret authentication information.
	Additional technical information on the Control	The main methods for using secret authentication information are using biometrics of the user directly, using devices such as IC cards, which contain the secret authentication information, and using the passwords. Technical assessment for the users is necessary for the password management in the three methods. In order to prevent from an unauthorized access to the computer resources, the password should be created and kept secret from those not allowed to access to them. Password authentication is the method of user authentication used by several resources such as operating systems, programs, databases, networks or web sites. The quality of passwords depends on the length and the type of characters such as alphanumeric characters and marks. It may be possible for users to configure the parameters of password policy to some operating systems such as Windows. On the other hand, the developers of applications may develop the authentication function to configure the password policy. Auditors should assess that the authorization functions with passwords are placed at the computer resources effectively, and those functions work appropriately.
	Security implementation standard	Select quality passwords with sufficient minimum length which are: 1) Easy to remember; 2) Not based on anything somebody else can easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth, etc.; 3) Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries); 4) Free of consecutive identical, all-numeric or all-alphabetic characters; 5) Different of previous passwords (take into account n generations).

ISO/IEC 27002:2013, 9.3 User responsibilities			
	Technical note on Security implementation standard	The passwords that are easy to remember for another user are vulnerable in general.	
1	1.1	Practice guide	Check that rule of password selection has been described in Organization's password policy.
		Evidence assumed	Organization's password policy
		Method	Examine/Review
	1.2	Practice guide	Check that setting of system configuration (System password policy) is as described in Organization's password policy.
		Evidence assumed	— System configuration (System password policy) — Organization's password policy
		Method	Examine/Observe
	1.3	Practice guide	Check that log file shows users have changed passwords
		Evidence assumed	Log file
		Method	Examine/Observe

ISO/IEC 27002:2013, 9.4 System and application access control		
	Control	**ISO/IEC 27002:2013, 9.4.1, Information access restriction** Access to information and application system functions should be restricted in accordance with the access control policy.
	Control	**ISO/IEC 27002:2013, 9.4.2, Secure log-on procedures** Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.
	Control	**ISO/IEC 27002:2013, 9.4.3, Password management system** Password management systems should be interactive and should ensure quality passwords.
	Control	**ISO/IEC 27002:2013, 9.4.4, Use of privileged utility programs** The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.
	Control	**ISO/IEC 27002:2013, 9.4.5, Access control to program source code** Access to program configuration files should be restricted and configuration file should be encrypted

B.2.6 ISO/IEC 27002:2013, Clause 10 Cryptography

ISO/IEC 27002:2013, 10.1 Cryptographic controls			
	Control	**ISO/IEC 27002:2013, 10.1.1, Policy on the use of cryptographic controls** A policy on the use of cryptographic controls for protection of information should be developed and implemented.	
	Additional technical information on the Control	Cryptography is a tool to protect information in computing systems and communications. Cryptographic systems are an integral part of standard protocols, most notably the Transport Layer Security (TLS) protocol, making it easy to incorporate strong encryption into a wide range of applications. Those cryptographic controls can be used to achieve different information security objectives, including: 1) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted; 2) integrity: cryptographic hash-functions can be used to verify the integrity of information; 3) authentication: Cryptographic protocols can be used to authenticate users and systems, requesting access for a resource; 4) authenticity: non-repudiation of communications or information can be achieved using cryptographic techniques like signature algorithms. To protect information, it should be determined which threats should be prevented through the use of cryptography.	
1	Security implementation standard	Cryptographic algorithms have an inherent complexity which impedes the secure usage of cryptographic controls. While implementing those controls, it must be insured to: 1) use a sufficient key length; 2) use protocols which are considered strong; 3) use of cryptographic algorithm which are considered to be strong; 4) use of implementations which are tested and known to be secure; 5) continuous evaluation.	
	Technical note on Security implementation standard	The implementation of cryptographic controls should be done by using strong and tested algorithms and implementations. It's not recommended to use internally-developed cryptographic algorithms and implementations.	
	1.1	Practice guide	Check that network services with implemented cryptographic controls have a sufficient key length and do not utilize weak algorithms.
		Evidence assumed	— Standard encryption methods — Access to encrypted services
		Method	Test and Validate
	1.2	Practice guide	Check that the used implementations for cryptographic controls are considered to be secure
		Evidence assumed	— Implementations of cryptographic controls — Version control mechanism for the used implementations
		Method	Test and Validate
	1.3	Practice guide	Check that mobile and removable media devices are protected with cryptographic controls using strong algorithms and sufficient key length.

ISO/IEC 27002:2013, 10.1 Cryptographic controls			
		Evidence assumed	— Standard encryption methods — Access to mobile media devices
		Method	Test and Validate
	1.4	Practice guide	Check that all cryptographic keys are stored safely and secure and can only be accessed by authorized persons
		Evidence assumed	— Access control methods for cryptographic keys — store process for cryptographic keys
		Method	Test and Validate
	1.5	Practice guide	Check that communication services with implemented cryptographic controls have a sufficient key length and do not utilize weak algorithms.
		Evidence assumed	— Standard encryption methods — Access to encrypted services — Access to Cryptographic Communication Information (e.g. Certificates)
		Method	Test and Validate
	Control	**ISO/IEC 27002:2013, 10.1.2, Key management** A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	

B.2.7 ISO/IEC 27002:2013, Clause 11 Physical and environmental security

ISO/IEC 27002:2013, 11.1 Secure areas		
	Control	**ISO/IEC 27002:2013, 11.1.1, Physical security perimeter** Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
	Control	**ISO/IEC 27002:2013, 11.1.2, Physical entry controls** Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
	Control	**ISO/IEC 27002:2013, 11.1.3, Securing offices, rooms and facilities** Physical security for offices, rooms and facilities should be designed and applied.
	Control	**ISO/IEC 27002:2013, 11.1.4, Protecting against external and environmental threats** Physical protection against natural disasters, malicious attack or accidents should be designed and applied.
	Control	**ISO/IEC 27002:2013, 11.1.5, Working in secure areas** Procedures for working in secure areas should be designed and applied.
	Control	**ISO/IEC 27002:2013, 11.1.6, Delivery and loading areas** Access points such as delivery and loading areas and other points where unauthorized persons can enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

ISO/IEC 27002:2013, 11.2 Equipment		
	Control	**ISO/IEC 27002:2013, 11.2.1, Equipment siting and protection** Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
	Control	**ISO/IEC 27002:2013, 11.2.2, Supporting utilities** Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.
	Control	**ISO/IEC 27002:2013, 11.2.3, Cabling security** Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.
	Control	**ISO/IEC 27002:2013, 11.2.4, Equipment maintenance** Equipment should be correctly maintained to ensure its continued availability and integrity.
	Control	**ISO/IEC 27002:2013, 11.2.5, Removal of assets** Equipment, information or software should not be taken off-site without prior authorization.
	Control	**ISO/IEC 27002:2013, 11.2.6, Security of equipment and assets off-premises** Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.
	Control	**ISO/IEC 27002:2013, 11.2.7, Secure disposal or re-use of equipment** All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
	Control	**ISO/IEC 27002:2013, 11.2.8, Unattended user equipment** Users should ensure that unattended equipment has appropriate protection.
	Control	**ISO/IEC 27002:2013, 11.2.9, Clear desk and clear screen policy** A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted

B.2.8 ISO/IEC 27002:2013, Clause 12 Operations security

ISO/IEC 27002:2013, 12.1 Operational procedures and responsibilities		
	Control	**ISO/IEC 27002:2013, 12.1.1, Documented operating procedures** Operating procedures should be documented and made available to all users who need them.
	Control	**ISO/IEC 27002:2013, 12.1.2, Change management** Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.
	Control	**ISO/IEC 27002:2013, 12.1.3, Capacity management** The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
	Control	**ISO/IEC 27002:2013, 12.1.4, Separation of development, testing and operational environments** Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment. Development and testing environment should have anonymized data to reduce the risks to have indication on operational data.

ISO/IEC 27002:2013, 12.2		Protection from malware	
	Control	**ISO/IEC 27002:2013, 12.2.1, Controls against malware** Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	
	Additional technical information	Malware is a generic term used to refer to a code including a software, program, script that is designed to damage a computer system by means of stealing information, fraud, espionage, sabotage, and vandalism. When malware has been introduced into a computer system, the system may be damaged, or the information of the system may be stolen. It is also possible that its behaviour will damage other systems. Malware includes computer viruses, worms, Trojan horses, bot, spyware, dishonest adware, and other malicious and unwanted software. Under the condition of connecting organization network to the Internet, information security auditors should review that the detection/prevention functions of malware are placed at the boundary of the Internet comprehensively and effectively, and those functions work appropriately. Especially, to review whether the detection/prevention functionality is working appropriately, information security auditors have to confirm whether the pattern files or signatures used to detect malware have been updated. Some of the detection/prevention systems are architected to detect malware by using the pattern files or signatures, and some of them are architected to detect abnormal behaviour of the computer system without using any pattern files or signatures. Since there are some patterns to connect to the Internet such as connecting organization network to the Internet via the gateway or connecting each PC to the Internet directly, information security auditors should ensure that the detection/prevention system works appropriately under each circumstance. NOTE Information security auditors should be aware that the ability of detection/prevention system is limited for unknown malware such as Zero day attack.	
1	Security implementation standard	Installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the checks carried out should include: 1) Checking any files on electronic or optical media, and files received over networks, before use; 2) Checking electronic mail attachments and downloads before use; this check should be carried out at different places, e.g. at electronic mail servers, desktop computers and when entering the network of the organization; 3) Checking web pages.	
	Technical note on security implementation standard	At the gateway, the entrance of the organization's network, the detection/prevention system of malware should work appropriately for a variety of services or protocol over networks such as WWW, Mail and FTP.	
	1.1	B.2.8.1 Practice guide	Following Practice guides are applied for 'Security implementation standard' 1), 2), and 3), respectively. 1) Check that detection of malicious code and repair system is placed comprehensively and effectively for any files on electronic or optical media, and files received over networks by reviewing the system specification or network diagrams. Information security auditors should check that the detection/prevention system is placed comprehensively and effectively by reviewing the system specification or network diagrams.

ISO/IEC 27002:2013, 12.2 Protection from malware			
			2) Check that detection of malicious code and repair system is placed comprehensively and effectively for any electronic mail attachments and downloads by reviewing the system specification or network diagrams which include electronic mail servers, desktop computers, and the gateway. The detection of malicious code and repair system is sometimes clearly described in the system specification as an exclusive device, however, information security auditors note that it is also placed in the servers which are designed to provide some other functions/ services (WWW, Mail, and FTP) and thus it locates inherently in the system specification without clear description. For desktop PCs, information security auditors note that the detection of malicious code and repair system locates inherently in the system specification without clear description. 3) Check that detection of malicious code and repair system is placed comprehensively and effectively for web pages by reviewing the system specification or network diagrams which include web server. For desktop PCs, which are used for reviewing or browsing web pages, information security auditors note that the detection of malicious code and repair system locates inherently in the system specification without clear description. In this case, the detection of malicious code and repair system may locate inherently in browser. For web server, the detection of malicious code and repair system is sometimes clearly described in the system specification as an exclusive device, however, information security auditors note that it is also placed in the web servers inherently in the system specification without clear description.
		Evidence assumed Method	— Contractual document, — Network service design document, — System specification, — Network diagram, — Examine/Review.
	1.2	Practice guide	Following Practice guides are applied for 'Security implementation standard' 1), 2), and 3) respectively. 1) Check that detection of malware and repair system is placed, and it is working appropriately for detecting any files on electronic or optical media, and files received over networks by observing the information processing facilities. Check whether management software is working appropriately in the integrated system under the circumstance where detection of malware and repair system is managed into an integrated system.

ISO/IEC 27002:2013, 12.2 Protection from malware			
			2) Check that detection of malware and repair system is placed, and it is working appropriately for detecting any electronic mail attachments and downloads at electronic mail servers, sampled desktop computers, and the gateway by observing the information processing facilities. For electronic mail, check that detection system works not only for attachment files but also malware in the html mail. 3) Check that detection of malware and repair system is placed, and it is working appropriately for detecting any web pages by observing the information processing facilities. For desktop PCs which are used for reviewing or browsing web pages, check that detection system works for unauthorized Active X control, scripts, etc. For web server, check that detection system works not only for html files but also the malware in the web services such as apache, IIS, etc.
		Evidence assumed Method	Facilities of detection of malware and repair system is placed, for example: — File server; — E-mail server; — Sampled desktop PCs; — Mobile computers; — An exclusive d detection of malware and repair system placed at the gateway (boundary between organizational network and the Internet); — Web server; — PROXY server; — Web browser; — Others (the device to block USB to be inserted physically); — Examine/Observe.
	1.3	Practice guide	Collect log files from the detection and repair system and check that the records of the logs show that the system has been running and the necessary action has been taken when malware has been detected. Check that detection of malware and repair system is placed comprehensively and effectively for web pages by uploading the EICAR test virus. NOTE For desktop PCs, the typical output logs from the detection and repair system are stored in the PCs. For servers and external devices, those logs are sometime transferred and stored in other systems via transferring protocol such as syslog. For desktop PCs, which are used for reviewing or browsing web pages, the detection function in the web browser may not produce records of the logs, which shows that the function has been running. Rather most of the browser shows the message when unauthorized scripts are detected.

ISO/IEC 27002:2013, 12.2 Protection from malware			
		Evidence assumed Method	— The detection system in service, — Log files output from detection system, — Records of detection system alert, — Message from detection system in web browser, — Web server with upload function in web browser, — Examine/Observe, — Test and Validate.
2	Security implementation standard	Malware detection and repair software to scan computers and media as a precautionary control should be regularly updated or on a routine basis.	
	Technical note on security implementation standard	In most cases, there are functions to update pattern files or signatures automatically.	
	2.1	B.2.8.2 Practice guide	Check the design of Malware detection and repair software to update the pattern files or signatures automatically or on a routine base.
		Evidence assumed	The design or specification of detection system
		Method	Examine/Review
	2.2	Practice guide	Check that setting of Malware detection and repair software to update the pattern files or signatures automatically or on a routine base.
		Evidence assumed	The setting of detection system
		Method	Examine/Observe
	2.3	Practice guide	Check that pattern files or signatures have been updated via observing the product name, version and the update log of their pattern files or signatures. NOTE Information of product name and its version of detection and repair system may be observed in the help file of the product.
		Evidence assumed	Information of detecting/preventing system, i.e.: — Name of product; — Version of the product; — Version of the pattern file or signature.
		Method	Examine/Observe

ISO/IEC 27002:2013, 12.3 Backup			
	Control	**ISO/IEC 27002:2013, 12.3.1, Information backup** Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.	
	Additional technical information on the Control	To take backup appropriately, organization standard should be defined in accordance with backup policy and it should be reflected to backup design document. Backups are used to recover the essential information or software in case of a data loss event such as a disaster or a media failure. When an organization designs backup, adequate backup site, backup path and backup method should be selected in accordance with the organization's backup policy. In terms of backup site, the organization should select whether onsite or offsite as a backup site. Onsite backup is considered to be much faster as compared to offsite backup to take backup and restore. Offsite backup is often selected in order to prevent from the influence of local disasters such as fires, floods, or earthquakes. In terms of backup path, whether online or offline should be selected. Online backup means that data is backed up via network or communication line. Offline backup means that backed-up data is physically transported with removable media such as DLTs or CD/DVDs. Backup method is classified several options such as full backup, incremental backup and differential backup. Full backup means backup of all the data that are selected to be backed up are taken. It will need more time and data capacity than the other methods, but it is the most simple and easiest method to restore. Incremental backup means to take backup the data that have changed since the last backup. It will need less time and data capacity than the other methods, but it is the most complicated method to restore. Differential backup means to take backup the data that have changed since the last full backup. It will need less time and data capacity than full backup and more simple and easier method to restore than incremental backup.	
1	Security implementation standard	The extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization.	
	Technical note on Security implementation standard	In accordance with the business requirement, the organization should select the adequate backup/restore time and data capacity for backups. Auditors should assess that the adequate backup method is selected to satisfy the business requirement. Examples of frequency to be concerned are: — Mirroring or real time replication (when the criticality of the information is the highest level); — Daily (when the restoration of the data which is backed-up at least within a day is required); — Weekly; — Monthly.	
	1.1	Practice guide	Check that backup design is based on security implementation standard.
		Evidence assumed	— Backup specification document — Business and security requirements definition document — Backup design document

ISO/IEC 27002:2013, 12.3 Backup			
		Method	Examine/Review
	1.2	Practice guide	Check that setting of system configuration files for backup is as described in backup design document.
		Evidence assumed	— Backup design document — Backup system configuration files
		Method	Examine/Review
	1.3	Practice guide	Check that backup has been taken as documented in backup design document.
		Evidence assumed	— Backup design document — Log files — Backup media
		Method	Examine/Observe
	1.4	Practice guide	Check that backup is stored in **a secure** correctly sized and isolated location
		Evidence assumed	Backup location specification document
		Method	Examine/Review
2	Security implementation standard	Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.	
	Technical note on Security implementation standard	Complexity and required time for restoration differ by the methods taken; such as full or differential backup. Test and check plan of restoration procedures should be prepared and documented.	
	2.1	Practice guide	Check that test and check plan is regularly checked.
		Evidence assumed	Records of check on the test and check plan
		Method	Examine/Review
	2.2	Practice guide	Check that the test and check plan has been tested regularly to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
		Evidence assumed	— Records of recovery test — test and check plan
		Method	Examine/Review

ISO/IEC 27002:2013, 12.4		Logging and monitoring
	Control	**ISO/IEC 27002:2013, 12.4.1, Event logging** Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.
	Additional technical information on the Control	To detect unauthorized information processing activities, it is important to record the audit logs that are used to trace the activities of users, system operators, security events and systems. The audit logs should contain the following information in order to analyse whether unauthorized activities, security events are occurred: — user IDs; — date and time; — key events such as log-on and log-off; — terminal identity; — network address and protocols.
		In order to produce the necessary record including the above information, the equipment, which produce the logs, should have been tuned up or some rules are applied to them. The method of logging depends on system structure, architecture and implemented applications. Information security auditors should take into account the difference of logging method for different system architecture such as servers and PCs. NOTE Examples of the System structures to be concerned are: — Client Server system; — Web-based system; — Thin client system; — Virtualization; — Utilization of ASP (Application Service Provider), SaaS (Software as a Service) or Cloud Computing. Examples of the System architectures to be concerned are: — UNIX, Linux; — Windows; — Mainframe; — Examples of the Log types to be concerned are: — System log; — Application log.

ISO/IEC 27002:2013, 12.4 Logging and monitoring			
1	Security implementation standard	Audit logs recording user activities, exceptions, and information security events should be produced. Audit logs should include, when relevant: a) user IDs; b) dates, times and details of key events, e.g. log-on and log-off; c) terminal identity or location if possible; d) records of successful and rejected system access attempts; e) records of successful and rejected data and other resource access attempts; f) changes to system configuration; h) use of system utilities and applications; i) files accessed and the kind of access; j) network addresses and protocols; k) alarms raised by the access control system; l) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.	
	Technical note on Security implementation standard	In accordance with the business requirement, the organization should select the adequate backup/restore time and data capacity for backups. Auditors should assess that the adequate backup method is selected to satisfy the business requirement. Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken. Where possible, system administrators should not have permission to erase or deactivate logs of their own activities. Examples of frequency to be concerned are: — Mirroring or real time replication (when the criticality of the information is the highest level); — Daily (when the restoration of the data which is backed-up at least within a day is required); — Weekly; — Monthly.	
	1.1	Practice guide	Check that system design of logging is based on Security implementation standard.
		Evidence assumed	— Specification document — Requirement definition document — Software design document
		Method	Examine/Review
	1.2	Practice guide	Check that setting of system configuration files of logging is as described in system design documents.
		Evidence assumed	— Software design document — System configuration file
		Method	Examine/Review

ISO/IEC 27002:2013, 12.4 Logging and monitoring			
	1.3	Practice guide	Check the records of actual audit log files are as described in the system design documents. NOTE In the audit logs, there are some records, which appear constantly, and some of the records such as error records do not. To check whether the system records the records which appear only in some specific case, information security auditors may need to use various measures including producing the test case, checking a system design documents.
		Evidence assumed	— Log file
		Method	Examine/Observe
	1.4	Practice guide	In some cases, the storing periods of audit logs are defined by business purpose, contract, and law/regulations'. For example, the audit logs, which contain alarms raised by the access control system, should be stored until the investigation of the events, causality of incidents has been completed. NOTE Relatively young system of which operation has just begun, its audit logs have not been stored in the period of agreement. In such a case, to achieve the following Practice guide 2.3, the following Practice guide 2.1 and 2.2 are necessary to be checked.
		Evidence assumed	— Log file
		Method	Examine/Observe
2	Security implementation standard	Audit logs should be kept for an agreed period to assist in future investigations and access control monitoring.	
	Technical note on Security implementation standard	In some cases, the storing periods of audit logs are defined by business purpose contract and law/regulations. For example, the audit logs, which contain alarms raised by the access control system, should be stored until the investigation of the events, causality of incidents has been completed. NOTE Relatively young system of which operation has just begun, its audit logs have not been stored in the period of agreement. In such a case, to achieve the following Practice guide 2.3, the following Practice guide 2.1 and 2.2 are necessary to be checked.	
	2.1	Practice guide	Check the storing period of audit logs is as described in system design documents.
		Evidence assumed	— Log file — System design document
		Method	Examine/Review
	2.2	Practice guide	Check the setting of the storing period of audit logs in the system are as described in system design documents, or the setting of overwriting nor erasing the audit logs before the storing period is not applied.
		Evidence assumed	— Log file — System design document
		Method	Examine/Review
	2.3	Practice guide	Check the storing period of audit logs is longer than the period agreed by observing the timestamps of log files or time record in the log.
		Evidence assumed	— Log file — System design document
		Method	Examine/Review

ISO/IEC 27002:2013, 12.4 Logging and monitoring			
	Control	**ISO/IEC 27002:2013, 12.4.2, Protection of log information** Logging facilities and log information should be protected against tampering and unauthorized access.	
	Additional technical information on the Control	System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the copying of appropriate message types automatically to a second log, or the use of suitable system utilities or audit tools to perform file interrogation and rationalisation should be considered.	
1	Security implementation standard	Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility.	
	Technical note on Security implementation standard	— System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security. Real-time copying of logs to a system outside the control of a system administrator or operator can be used to safeguard logs.	
	1.1	Practice guide	Check that only authorized and privileged users can access log files. Both read and write access should be restricted to privileged users.
		Evidence assumed	— Access to log server — Access to logs — A privileged and an unprivileged user account
		Method	Test and Validate
	1.2	Practice guide	Check that all log files are transmitted over a secure connection to the management system (i.e. logging server or SIEM)
		Evidence assumed	— Access to log server — Access to network services used for transmitting log information
		Method	Test and Validate
	1.3	Practice guide	Check that all changes in log files can be tracked by a management system
		Evidence assumed	— Access to the log management system — Access to log files
		Method	Test and Validate
	1.4	Practice guide	Check that all unprivileged or unexpected changes in log files can be identified.
		Evidence assumed	— Use of Hashes/Signatures — Access to Log Management
		Method	Test and Validate
	1.5	Practice guide	Check that privileged and authenticated users cannot manipulate their own log files.
		Evidence assumed	— Privileged user account — Access to log management
		Method	Test and Validate
	1.6	Practice guide	Check that users can only access log files that match with their privileges.
		Evidence assumed	— Access to log management system — Access to logs — Access to two user accounts with differing privileges

ISO/IEC 27002:2013, 12.4 Logging and monitoring			
		Method	Test and Validate
	1.7	Practice guide	Check that all changes in log files can be tracked by a management system
		Evidence assumed	Check that log files are sufficiently encrypted.
		Method	Test and Validate
	1.8	Practice guide	Check that unauthorized access to the log management system is strictly prohibited.
		Evidence assumed	— Network access to log management system
		Method	Test and Validate
	1.9	Practice guide	Verify the unprivileged access to alarm, log, and notification storage locations and property.
		Evidence assumed	— Access to the log management system — Access to log files
		Method	Test and Validate
2	Security implementation standard	Audit logs should be kept for an agreed period to assist in future investigations and access control monitoring.	
	Technical note on Security implementation standard	In some cases, the storing periods of audit logs are defined by business purpose contract and low/regulations'. For example, the audit logs, which contain alarms raised by the access control system, should be stored until the investigation of the events, causality of incidents has been completed. NOTE Relatively young system of which operation has just begun, its audit logs have not been stored in the period of agreement. In such a case, to achieve the following Practice guide 2.3, the following Practice guide 2.1 and 2.2 are necessary to be checked.	
	Control	**ISO/IEC 27002:2013, 12.4.4, Clock synchronisation** The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.	

ISO/IEC 27002:2013, 12.5 Control of operational software		
	Control	ISO/IEC 27002:2013, 12.5.1, Installation of software on operational systems Procedures should be implemented to control the installation of software on operational systems.

ISO/IEC 27002:2013, 12.6 Technical vulnerability management		
	Control	**ISO/IEC 27002:2013, 12.6.1, Management of technical vulnerabilities** Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
	Control	**ISO/IEC 27002:2013, 12.6.2, Restrictions on software installation** Rules governing the installation of software by users should be established and implemented.

ISO/IEC 27002:2013, 12.7 Information systems audit considerations		
	Control	**ISO/IEC 27002:2013, 12.7.1, Information systems audit controls** Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.

B.2.9 ISO/IEC 27002:2013, Clause 13 Communications security

ISO/IEC 27002:2013, 13.1	Network security management		
	Control	**ISO/IEC 27002:2013, 13.1.1, Network controls** Networks should be managed and controlled to protect information in systems and applications.	
	Additional technical information on the Control	Network service is the service, which is provided on the networked computing environment whether it is in-house or outsourced. When an organization uses the network services, confidential information of the organization may be transmitted in way of outsourced network service. So, auditors should take into account that the necessary security functions such as encryption and/or authentication are provided by the outsourced network service provider. Example of systems used for network service are: — DNS — DHCP — Firewall/VPN — Anti Virus detector — IDS/IPS	
1	Security implementation standard	The security arrangements necessary for particular services, such as security features, service levels, and management requirements should be identified. The organization should ensure that network service providers implement these measures.	
	Technical note on Security implementation standard	To use network service, security arrangement is important to protect information passing over it. Requirements about security features are typically included in business requirements. Examples of security features related to network service are depicted as follows; — Encryption against eavesdropping, — Network access control against unauthorized access, — IDS/IPS against malicious activities, — URL filtering against unauthorized WEB access, and — Incident response for unexpected security events.	
	1.1	B.2.9.1 Practice guide	Check that contractual document including SLA (Service Level Agreement) provided from service provider satisfies the organization's business, legal, and security requirements.
		Evidence assumed	— Contractual document — Requirement definition document
		Method	Examine/Review
	1.2	B.2.9.2 Practice guide	In case of in-house, check that the setting of system used for network service is as described in network service design document.
		Evidence assumed	— System Configuration — Network service design document
		Method	Examine/Review

ISO/IEC 27002:2013, 13.1	**Network security management**		
	1.3	B.2.9.3 Practice guide	In case of in-house, check the records of actual log files from network service systems are as described in the network service design documents. Example of records of network service: — Authentication; — Encryption; — Network connection controls; — Speed of circuit; — Response (In case of on-line system); — Length of downtime
		Evidence assumed	— Log files — Alert message — Network service design document
		Method	Examine/Observe
	Control	**ISO/IEC 27002:2013, 13.1.2, Security of network services** Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.	
	Additional technical information on the Control	Network service is the service, which is provided on the networked computing environment whether it is in-house or outsourced. When an organization uses the network services, confidential information of the organization may be transmitted in way of outsourced network service. So, auditors should take into account that the necessary security functions such as encryption and/or authentication are provided by the outsourced network service provider. Example of systems used for network service are: — DNS (Domain Name System) — DHCP (Dynamic Host Configuration Protocol) — Firewall/VPN (Virtual Private Network) — Anti Virus IDS/IPS (Intrusion detection system/Intrusion prevention system)	
1	Security implementation standard	The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed. The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The organization should ensure that network service providers implement these measures.	
	Technical note on Security implementation standard	Network services include the provision of connections, private network services and value added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.	
	1.1	Practice guide	Verify that security mechanisms included in network services agreements are regularly tested and validated.
		Evidence assumed	— Access to network service agreements — Access to security test reports
		Method	Examine

ISO/IEC 27002:2013, 13.1	**Network security management**		
	1.2	Practice guide	Verify that the IDS/IPS recognizes various automated attacks as well as manual malicious activities.
		Evidence assumed	— IDS/IPS is implemented — Access to IDS/IPS logs
		Method	Test and Validate
	1.3	Practice guide	In case of in-house, check the records of actual log files from network service systems are as described in the network service design documents. Example of records of network service: — Authentication; — Encryption; — Network connection controls; — Speed of circuit; — Response (In case of on-line system); — Length of downtime.
		Evidence assumed	— Access to a test separate test environment — Documented anti-virus / malware protection policy
		Method	Test and Validate
	1.4	Practice guide	Verify that access to VPN and other remote access mechanisms is properly restricted through authentication testing and environment breakout testing techniques.
		Evidence assumed	— VPN and/or other remote access services are implemented which allow access to the network — List of remote access points
		Method	Test and Validate
	Control	**ISO/IEC 27002:2013, 13.1.3, Segregation in networks** Groups of information services, users and information systems should be segregated on networks.	
	Additional technical information on the Control	One method of managing the security of large networks is to divide them into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks (e.g. virtual private networking).	
1	Security implementation standard	The perimeter of each domain should be well defined. Access between network domains is allowed, but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the access control policy (see 9.1.1), access requirements, value and classification of information processed and also take account of the relative cost and performance impact of incorporating suitable gateway technology. Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, consideration should be made to treat all wireless access as external connections (see 9.4.2) and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls policy (see 13.1.1) before granting access to internal systems.	

ISO/IEC 27002:2013, 13.1		Network security management	
	Technical note on Security implementation standard	Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organization's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.	
	1.1	Practice guide	Validate that virtually segregated networks cannot be reached through ping scanning, VLAN hopping and/or the introduction of new virtual interfaces.
		Evidence assumed	— Network segregation through VLANs
		Method	Test and Validate
	1.2	Practice guide	Test firewalls to confirm that attackers cannot access unauthorized networks and that control points are not susceptible to common vulnerabilities.
		Evidence assumed	— Networks are segregated by firewalls
		Method	Test and Validate
	1.3	Practice guide	Validate that systems with network interfaces in separate networks regularly receive security updates and are not vulnerable to common vulnerabilities. Vulnerable systems with interfaces in multiple networks can be used to pivot to other restricted networks.
		Evidence assumed	— Documentation listing all wireless networks
		Method	Test and Validate
	1.4	Practice guide	Validate that there are no existing rogue access points on the premises that are undocumented and may grant access to normally segregated networks.
		Evidence assumed	— Documentation listing all wireless networks
		Method	Test and Validate

ISO/IEC 27002:2013, 13.2		Information transfer
	Control	**ISO/IEC 27002:2013, 13.2.1, Information transfer policies and procedures** Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.
	Control	**ISO/IEC 27002:2013, 13.2.2, Agreements on information transfer** Agreements should address the secure transfer of business information between the organization and external parties.
	Control	**ISO/IEC 27002:2013, 13.2.3, Electronic messaging** Information involved in electronic messaging should be appropriately protected.
	Control	**ISO/IEC 27002:2013, 13.2.4, Confidentiality or non-disclosure agreements** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.

B.2.10 ISO/IEC 27002:2013, Clause 14 System acquisition, development and maintenance

ISO/IEC 27002:2013, 14.1 Security requirements of information systems			
	Control	**ISO/IEC 27002:2013, 14.1.1, Information security requirements analysis and specification** The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.	
	Control	**ISO/IEC 27002:2013, 14.1.2, Securing application services on public networks** Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	
	Additional technical information on the Control	Communication between a client and an application service should be handled securely. This can be done by: 1) using authentication 2) using documented processes for approving content 3) ensuring that communicating partners are fully informed of their authorizations for the use of the service 4) determining that all communication parties fulfill all security requirements 5) using mechanisms to ensure the communication and its information is integer, confidential, and authentic — Most of these requirements can be achieved by using cryptographic controls (A.10). Legal aspects should be handled in service agreements.	
1	Security implementation standard	The security of application services on public networks is closely related to cryptographic controls. These controls can be used to achieve many of the goals described above. The authentication and authorization can be achieved by using well known and trusted authentication protocols. To ensure the communication between a client and an application service over a public network is confident, this service can be secured by using known public key cryptography for key exchange and symmetric cryptography, like Block — or Stream-Ciphers, for encryption. The integrity of the communication over a public network can be reached by using strong cryptographic signature algorithms.	
	Technical note on Security implementation standard	To ensure that the application service on a public network is secure against various forms of threats and attacks, it should be determined that all cryptographic protocols and algorithms fulfill the controls defined in A.10 Cryptographic Controls. Applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public. Therefore, detailed risk assessments and proper selection of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.	
	1.1	Practice guide	Check that the authentication and authorization information and processes are implemented using strong, well known, and tested protocols and algorithms.
		Evidence assumed	— Access to the implemented authentication and authorization process — Access to the algorithms and protocols — Valid authentication information
		Method	Test and Validate
	1.2	Practice guide	Verify that the application is resistant against various protocol level threats and attacks.

ISO/IEC 27002:2013, 14.1 Security requirements of information systems			
		Evidence assumed	— Access to the communication protocol — Access to the communication channel
		Method	Test and Validate
	1.3	Practice guide	Verify that the communication is resistant against various application level threats and attacks such as code injection, privilege escalation, session hijacking and insecure direct object references.
		Evidence assumed	— Non-privileged access to the application — Privileged access to the application
		Method	Test and Validate
	1.4	Practice guide	Enumerate and test for use or inadequacies from monitors and sensors to properly identify and log access or interactions with assets for specific evidence to challenge repudiation. Document the depth of the interaction which is recorded.
		Evidence assumed	— Access to logs and monitoring system
		Method	Examine
	1.5	Practice guide	Verify that all methods of interaction are properly recorded with proper identification.
		Evidence assumed	— Access to logs and monitoring system
		Method	Examine
	1.6	Practice guide	Verify that application logs cannot be deleted by application users.
		Evidence assumed	— Access to application
		Method	Test and Validate
	Control	**ISO/IEC 27002:2013, 14.1.3, Protecting application services transactions** Information involved in application service transactions should be protected to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	
	Additional technical information on the Control	Protecting application services transactions is an important factor when implementing and maintaining security relevant services. Those services use information for authentication, system control or general communication. This information can include login credentials, system commands, private information or much more, which need to be protected. Information needed in application services should be protected against various attacks and threats.	
1	Security implementation standard	To protect information transmitted to an application service, it is recommended to ensure to: 1) use digital signatures for each involved party; 2) use encryption on the communication path between all involved parties; 3) use protocols that are tested and known to be secure; 4) use protocols that ensure that the transaction remains valid, confidential and private; 5) use a system which is not publicly accessible to store transaction details.	
	Technical note on Security implementation standard	The extent of the controls adopted needs to be commensurate with the level of the risk associated with each form of application service transaction.	

ISO/IEC 27002:2013, 14.1 Security requirements of information systems			
	1.1	Practice guide	Validate that all SSL certificates are valid and issued from a trustworthy certificate authority for the specific organization.
		Evidence assumed	— SSL certificate in use — Access to the application service
		Method	Test and Validate
	1.2	Practice guide	Check that the communication between all parties is encrypted using strong cryptographic algorithms with a sufficient key length.
		Evidence assumed	— Standard encryption methods and key length — Access to encrypted communication
		Method	Test and Validate
	1.3	Practice guide	Verify that the communication is resistant against various application level threats and attacks such as cross-site scripting, cross-site request forgery and invalidated redirects and forwards.
		Evidence assumed	— Non-privileged access to the application — Privileged access to the application
		Method	Test and Validate
	1.4	Practice guide	Test whether the application or protocol implementation are vulnerable to known attacks like man-in-the-middle or replay attacks.
		Evidence assumed	— Access to communication — Standard Communication Protocols
		Method	Test and Validate
	1.5	Practice guide	Validate that all confidential data saved by the application is stored securely.
		Evidence assumed	— Access to the application database
		Method	Test and Validate
	1.6	Practice guide	Validate that external access to the database is prohibited and all access is restricted through secure authentication mechanisms.
		Evidence assumed	— Access to the application database
		Method	Test and Validate
	1.7	Practice guide	Validate that the transaction remains valid even if the connection is lost through miss-routing or incomplete transmissions.
		Evidence assumed	— Access to communication — Access to the application logs
		Method	Test and Validate
	1.8	Practice guide	Validate that only minimal rights are used by the application. Ensure there are no more rights than needed.
		Evidence assumed	Access to application's database user information
		Method	Test and Validate

ISO/IEC 27002:2013, 14.2 Security in development and support processes		
	Control	**ISO/IEC 27002:2013, 14.2.1, Secure development policy** Rules for the development of software and systems should be established and applied to developments within the organization.
	Control	**ISO/IEC 27002:2013, 14.2.2, System change control procedures** Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.
	Control	**ISO/IEC 27002:2013, 14.2.3, Technical review of applications after operating platform changes** When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
	Control	**ISO/IEC 27002:2013, 14.2.4, Restrictions on changes to software packages** Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.
	Control	**ISO/IEC 27002:2013, 14.2.5, Secure system engineering principles** Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.
	Control	**ISO/IEC 27002:2013, 14.2.6, Secure development environment** Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
	Control	**ISO/IEC 27002:2013, 14.2.7, Outsourced development** The organization should supervise and monitor the activity of outsourced system development.
	Control	**ISO/IEC 27002:2013, 14.2.8, System security testing** Testing of security functionality should be carried out during development.
	Control	**ISO/IEC 27002:2013, 14.2.9, System acceptance testing** Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

ISO/IEC 27002:2013, 14.3 Test data		
	Control	**ISO/IEC 27002:2013, 14.3.1, Protection of test data** Test data should be selected carefully, protected and controlled.

B.2.11 ISO/IEC 27002:2013, Clause 15 Supplier relationships

ISO/IEC 27002:2013, 15.1 Information security in supplier relationships		
	Control	**ISO/IEC 27002:2013, 15.1.1, Information security policy for supplier relationships** Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.
	Control	**ISO/IEC 27002:2013, 15.1.2, Addressing security within supplier agreements** All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.
	Control	**ISO/IEC 27002:2013, 15.1.3, Information and communication technology supply chain** Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

ISO/IEC 27002:2013, 15.2 Supplier service delivery management		
	Control	**ISO/IEC 27002:2013, 15.2.1, Monitoring and review of supplier services** Organizations should regularly monitor, review and audit supplier service delivery.
	Control	**ISO/IEC 27002:2013, 15.2.2, Managing changes to supplier services** Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

B.2.12 ISO/IEC 27002:2013, Clause 16 Information security incident management

ISO/IEC 27002:2013, 16.1 Management of information security incidents and improvements		
	Control	**ISO/IEC 27002:2013, 16.1.1, Responsibilities and procedures** Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.
	Control	**ISO/IEC 27002:2013, 16.1.2, Reporting information security events** Information security events should be reported through appropriate management channels as quickly as possible.
	Control	**ISO/IEC 27002:2013, 16.1.3, Reporting information security weaknesses** Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.
	Control	**ISO/IEC 27002:2013, 16.1.4, Assessment of and decision on information security events** Information security events should be assessed and it should be decided if they are to be classified as information security incidents.
	Control	**ISO/IEC 27002:2013, 16.1.5, Response to information security incidents** Information security incidents should be responded to in accordance with the documented procedures.
	Control	**ISO/IEC 27002:2013, 16.1.6, Learning from information security incidents** Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.
	Control	**ISO/IEC 27002:2013, 16.1.7, Collection of evidence** The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

B.2.13 ISO/IEC 27002:2013, Clause 17 Information security aspects of business continuity management

ISO/IEC 27002:2013, 17.1 Information security continuity		
	Control	**ISO/IEC 27002:2013, 17.1.1, Planning information security continuity** The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
	Control	**ISO/IEC 27002:2013, 17.1.2, Implementing information security continuity** The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
	Control	**ISO/IEC 27002:2013, 17.1.3, Verify, review and evaluate information security continuity** The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

ISO/IEC 27002:2013, 17.2 Redundancies		
	Control	**ISO/IEC 27002:2013, 17.2.1, Availability of information processing facilities** Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

B.2.14 ISO/IEC 27002:2013, Clause 6 Compliance

ISO/IEC 27002:2013, 18.1 Compliance with legal and contractual requirements		
	Control	**ISO/IEC 27002:2013, 18.1.1, Identification of applicable legislation and contractual requirements** All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization.
	Control	**ISO/IEC 27002:2013, 18.1.2, Intellectual property rights** Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
	Control	**ISO/IEC 27002:2013, 18.1.3, Protection of records** Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.
	Control	**ISO/IEC 27002:2013, 18.1.4, Privacy and protection of personally identifiable information** Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.
	Control	**ISO/IEC 27002:2013, 18.1.5, Regulation of cryptographic controls** Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.

ISO/IEC 27002:2013, 18.2 Information security reviews		
	Control	**ISO/IEC 27002:2013, 18.2.1, Independent review of information security** The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.
	Control	**ISO/IEC 27002:2013, 18.2.2, Compliance with security policies and standards** Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security.
	Control	**ISO/IEC 27002:2013, 18.2.3, technical compliance review** Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.

Annex C
(informative)

Technical assessment guide for cloud services (Infrastructure as a service)

C.1 Positioning and purpose

This annex provides guidance for reviewing the implementation and operation of the controls and implementation guidance given in ISO/IEC 27017. This annex is assumed to be used as the additional guidance for that provided in Annex B, which addresses the controls, and implementation guidance given in ISO/IEC 27002.

The purpose of this annex is to provide a reviewer with understanding of review points specific to cloud services, assuming infrastructure as a service (see Figure C.1). The systems, which provide cloud services, are diverse and keep changing due to significant technology innovation. This annex does not assume a specific system but targets to be used as a practice for review methods, notes, and review targets.

In addition, this annex gives insights to the engineers of the cloud service provider, which would incorporate adopted security controls, to be reviewed how the service should be verified and the technical assessment trail should be shown. Following this guideline allows not only reviewers to work on a proper review but also the cloud service provider to design specific controls to make their own service comply with ISO/IEC 27017.

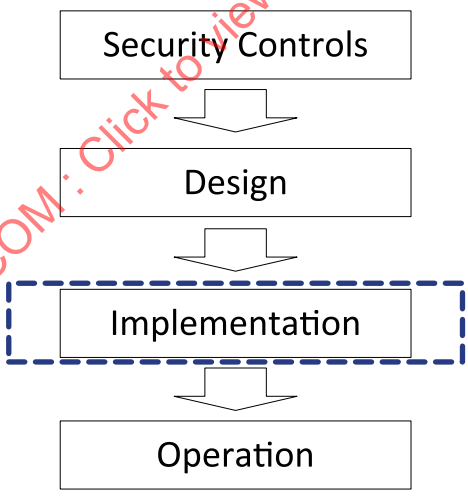

Figure C.1 — Scope of this annex

C.2 Relationship with other international standards

The following standards are related to this annex in addition to ISO/IEC 27017.

a) ISO/IEC 27018, which defines Personally Identifiable Information (PII) in cloud services.

   This annex covers infrastructure as a service. In infrastructure as a service, cloud service customers are responsible for their own information security on the information stored in a virtual machine used by the cloud service customers. This means that the cloud service provider is not able to administer PII in the virtual machine, causing this to be outside the scope of this document.

PII, which should be maintained by the cloud service provider, includes information on cloud service customers. This is managed by and stored in the Service management of the Implementation Model explained later. In addition, PII should be handled in the Service management according to ISO/IEC 27018.

b) ISO/IEC 17788, of which this annex applies overview and vocabulary on cloud computing.

c) ISO/IEC 17789, which applies for basic ideas on components which configure cloud services.

While ISO/IEC 17789 defines architecture of cloud computing in terms of its role and activities, cloud system implementation-conscious viewpoints are required in the review, including confirmation of a virtualization mechanism configuration.

Therefore, this annex presents the Implementation model which models a cloud system and maps functional components defined in ISO/IEC 17789 to review items.

C.3 Structure of this annex

This annex first suggests a cloud service environment modelling with infrastructure as a service assumed. This model describes the relationship between resource types and virtualization, and the concept of cloud service customers and tenant. Server, network and storage are identified as a resource type.

The technical assessment requirements are described in the same format as in Annex B in the order of common topics through the model, individual resource type and Service management.

See B.1 for the structure.

a) Explanation of the typical technologies

Explanation of technological elements and guideline related to virtualization implementation. When multiple implementation methods exist, typical methods are explained.

b) The controls defined in ISO/IEC 27017

Reference of the controls in ISO/IEC 27017, which related to the virtualization.

c) Technical assessment method for the controls of ISO/IEC 27017

Guideline of the review method for the controls of ISO/IEC 27017.

When multiple implementation methods exist, one of them is explained.

C.4 Cloud services (infrastructure as a service) environment model

C.4.1 Meaning of the model introduced

As cloud service technologies are diverse, dealing with them in detail, one by one, is too individual and specific. In addition, computing technologies used in the cloud service are new and still in the process of technical development. Considering this, standardizing technical assessment methods based on these individual/specific technologies is not appropriate. The information security auditor (or reviewer) can keep this methodological model in mind and recall whether the actual technologies implemented for a control have been designed based on the idea of the control and how evidences for assessment should be collected before the actual evaluation.

C.4.2 Model and components

In infrastructure as a service, as assumed in this annex, an environment is a precondition which provides cloud services consisting of:

a) virtual resources directly used by the cloud service customers;

b) virtualization mechanisms that install those resources; and

c) service management to control and provide the virtualization mechanisms.

Figure C.2 shows the Implementation Model for systems, which provide cloud services.

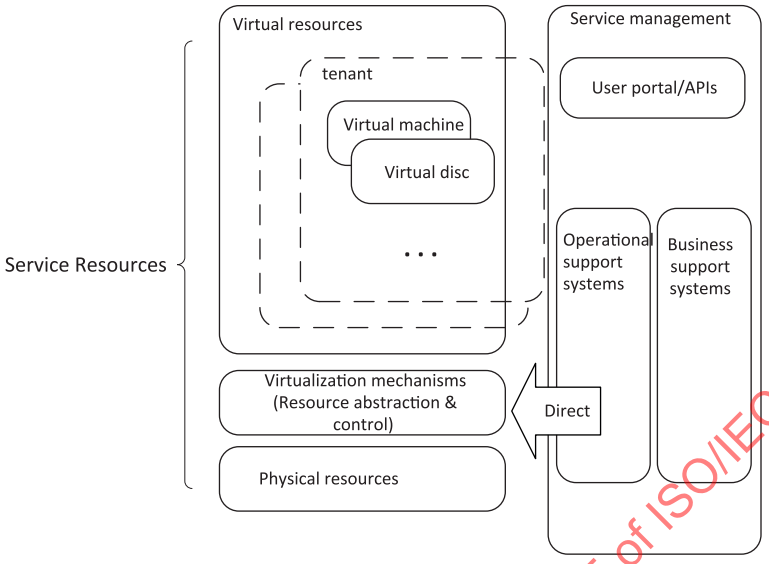

Figure C.2 — Implementation model

An important concept of this model is the virtualization and separation of the resource.

In the virtualization mechanisms, physical resources are provided as virtual resources with their access rights separated by tenant with resource abstraction and control components.

A tenant is an area where virtual resources allocated to each access controlled are aggregated. Multiple tenants can be provided to a cloud service customer by request. Generally, multiple users access a tenant and execute information processing.

This model has four components. Three of them, physical resources, virtualization mechanisms and virtual resources, are categorized into server, network and storage as resource types.

a) **Physical resources** are physical equipment required for providing cloud services. They consist of server equipment, network equipment, and storage equipment as components.

   The physical network equipment includes a physical Network Interface Card (NIC), which connects the server to the network. The physical storage equipment includes a Host Bus Adapter (HBA) and FC switches which connect the server to the storage.

b) **Virtualization mechanisms** are used to produce virtual resources provided by the cloud services. Hypervisor is applicable to this for a server virtualization. Virtual Local Area Network (VLAN) and Software Defined Network (SDN) apply for a network virtualization. Mostly storage devices include this mechanism for storage.

c) **Virtual resources** are created by the function for virtualization and are provided to cloud service customers in the cloud service such as virtual machines, virtual networks and virtual storages. "The virtual resources" indicate the concept of collection of resources virtually produced.

   NOTE Network and storage can be virtualized by servers. For instance virtualized switches configuring the virtual network can be created by Hypervisor, which virtualizes the server.

d) **Service management** is a system to enable the cloud service provider to provide cloud services, and provide an interface for the cloud system to the cloud service customer.

Using the above function for virtualization, it provisions virtual resources required for the cloud service. It also monitors and manages the physical resources and ensures to control that the entire cloud environment can function appropriately.

This Service management also includes portal functions, utilities, and Application Program Interfaces (APIs), which allow for cloud service customers to work on allowable operation, including provisioning and activation/deactivation of a VM.

C.4.3 Correspondence to ISO/IEC 17789

Functional components defined in ISO/IEC 17789 are actually implemented in this framework by implementation elements used to implement each component depending on the target resource type or layer.

Take Access Control as an example:

— Access control of physical disks Disk unit

— Access control per tenant Virtualization mechanisms

— Access control of virtual disks Virtualization mechanisms

— Access control in each VM OS of the VM

Multi-layer functions and components defined in ISO/IEC 17789, which serve cloud services, are included in the Service management in the Implementation Model of this annex. Business support systems (BSS) or operational support systems (OSS) defined in ISO/IEC 17789 are included in the Implementation Model of this annex.

Multi-layer functions in relation to integration and security are implemented in its target mechanisms as with the above access rights.

C.5 Common practice in the Implementation Model

C.5.1 General

This clause describes a checking practice common to server virtualization, network virtualization, and storage virtualization explained later.

C.5.2 Application of virtualization technologies in the cloud service

As explained above, virtualization consists of functions for virtualization and virtual resources. In infrastructure as a service, these virtual resources are to be accessed by cloud service users.

The following assessments are required for the virtualization mechanisms in a technical review of the cloud system:

a) Operations security

As operation of the virtualization mechanisms has direct impact on virtual resources, make sure that the operation is performed properly.

b) Definition of environment

Check if logs and events which need to be provided to cloud service customers (error notification, warning, and a value beyond the threshold, etc.) are defined as parameters of the virtualization mechanisms so that the information is collected and logged.

Check if redundancy of the virtualization mechanisms and virtual resources is also defined as parameters of the virtualization mechanisms and is to be reviewed regarding their availability.

c) Capacity management

In each virtualization, check if the relationship of virtual resources provided to cloud service customers with physical resources is managed.

In general, cloud computing provides logical resources available concurrently with a statistical approach. Therefore, the total virtual resources provided are larger than the total physical resources (oversubscription, overcommit).

C.5.3 Carrying out the technical assessment for the common aspects in the virtualization mechanism

C.5.3.1 Operation Security

Control	ISO/IEC 27017:2015, 12.1.2 Change management
Implementation guidance for cloud service provider	The cloud service provider should provide the cloud service customer with information regarding changes to the cloud service and the systems on which it runs that can adversely impact the cloud service customer's information security. The following will help the cloud service customer determine the effect the changes can have on information security: — Categories of changes; — Planned date and time of the changes; — Technical description of the changes to the cloud services and underlying systems; — Notification of the start and the completion of the changes. When a cloud service provider offers a cloud services that depends on a peer cloud service provider, then the cloud service provider can need to inform the cloud service customer of changes caused by the peer cloud service provider.
Additional technical information	Potentially significant changes for a cloud service customer are as shown below: Server: — Update or upgrade of Hypervisor — Changes in Hypervisor parameters and environmental definitions Network: — Changes in virtual LAN definitions — Changes in configuration, environment definitions and parameters of network devices including a switch, router, firewall and load balancer

Control		ISO/IEC 27017:2015, 12.1.2 Change management	
		Storage: — Changes in device definitions — Changes in SAN zoning, etc. Hardware: — Firmware upgrade Software: — Software upgrade — Application of program fixes (patches) — Application of security fixes These changes can have varied impacts on the cloud service customer. The cloud service customer and the cloud service provider should agree with the changes to be notified base on the level of impacts they have.	
1	Security implementation standard	In change management, cloud service customers who are directly or indirectly affected should be identified and notified appropriately.	
	Technical note on security implementation standard	As the IT resources are mutually dependent, cloud service customers using other resources, which are dependent on the relevant resources will be affected. In general, hardware and software configurations of the cloud service are maintained in the CMDB (Configuration Management Database). Hardware and software resources for each cloud service customer are also managed by CMDB, OSS (Operation Support System), or BSS (Business Support System). The relationship of hardware and software with the cloud service customers affected by the changes of that hardware and software is managed by these systems.	
	1.1	Practice guide	Check if cloud service customers who are using IT resources to be changed are identified.
		Evidence assumed	Search result of CMDB, etc. (Search result of cloud service customers who are utilizing specific IT resources specified.)
		Method	Examine/Observe
	1.2	Practice guide	Check if the relevant relationship is understood when dependencies or impacts between IT resources exist.
		Evidence assumed	Search result of CMDB, etc. (Search result of other IT resources affected by specific IT resources specified when dependencies exist between the IT resources.)
		Method	Examine/Observe
	1.3	Practice guide	Check if information on the change management, which should be provided to cloud service customers, is provided properly. Check the following on the information provided:
			— The changes are related to cloud service customers, and (Indirect impacts should also be provided.) — Agreements with customers or reasonably appropriate level of impacts are provided.
		Evidence assumed	Mail to cloud service customers Portal intended for cloud service customers
		Method	Examine/Observe

Control		ISO/IEC 27017:2015, 12.1.3 Capacity management	
Implementation guidance for cloud service provider		The cloud service provider should monitor the total capacity of computing resources to prevent information security incidents caused by resource shortages.	
Additional technical information		Computing resources provided by the cloud service provider should include: — CPU processing capacity, core memories — Network band — Storage capacity In the cloud system, the capacity management is mandatory to prevent computing resources from getting short at peak hours because a temporary use of computing resources involves the peak hours. The capacity management should be implemented not only across the cloud system but also in each block because the computing resources may not be provided beyond the block of the cloud system.	
1	Security implementation standard	Define a level beyond which computing resources should be added and take necessary actions when the level is reached.	
	Technical note on security implementation standard	Specify a certain threshold on computing resources and conduct monitoring to issue an alarm when the usage may exceed the threshold. Monitor the usage of the computing resources by using the cloud system, IT equipment, and software, etc.	
	1.1	Practice guide	Check if computing resources, which need the capacity management, are monitored as requirements.
		Evidence assumed	Definition of monitoring the cloud system Report output of the capacity usage
		Method	Examine/Observe
	1.2	Practice guide	Check if an alarm is issued when the capacity used exceeds the threshold.
		Evidence assumed	Alarm setting for the cloud monitoring system (check if an alarm is defined to be triggered by the threshold) Event log of the cloud monitoring system (check if an alarm was issued in the past)
		Method	Examine/Observe

Control		ISO/IEC 27017:2015, CLD.12.1.5 Administrator's operational security
Implementation guidance for cloud service provider		The cloud service provider should provide documentation about the critical operations and procedures to cloud service customers who require it.
Additional technical information		In general, if changes to the cloud computing environment fail, cloud service customers will be affected and prevented to use the cloud service. Especially, deletion and destruction of data on the storage are the most critical damage to customers' assets. It is assumed that a temporary service breakdown or the disabled cloud computing environment may not destroy the assets even if transactions being processed are discarded.
1	Security implementation standard	Only preauthorized operators are able to delete the data.
	Technical note on security implementation standard	Operation with administrative privileges with which data on the storage used by the cloud service customers can be deleted requires authentication different from that for the normal operation.

Control		ISO/IEC 27017:2015, CLD.12.1.5 Administrator's operational security	
	1.1	Practice guide	Check if IDs, which allow operation with administrative privileges, are limited and used with a different procedure than a normal one.
		Evidence assumed	List of user IDs including the storage operation utility, etc. Operation when using administrative privileges
		Method	Examine/Observe

Control		ISO/IEC 27017:2015, 12.4.1 Event logging	
Implementation guidance for cloud service provider		The cloud service provider should provide logging capabilities to the cloud service customer.	
Additional technical information		As described in ISO/IEC 27017 "Other information for cloud services", the cloud service provider is responsible for logging and monitoring cloud computing infrastructure components in IaaS covered in this document. They include: — Logs and events of Hypervisor — Logs and events of firewall and a load balancer — Logs and events of a storage device and SAN equipment As these infrastructure components are shared between cloud service customers, logs and events of all cloud service customers as a whole are logged. Therefore, a log only related to the relevant cloud service customer should be extracted and provided.	
1	Security implementation standard	A log to be provided to service customers is collected and events are monitored.	
	Technical note on security implementation standard	Cloud computing infrastructure components' function is used to output a log and collect events. Log output is defined by the definition of the cloud computing infrastructure components' parameters.	
	1.1	Practice guide	Check if log or event collection settings are defined for the cloud computing infrastructure components.
		Evidence assumed	Definition of the cloud computing infrastructure components' parameters
		Method	Examine/Observe

Control	ISO/IEC 27017:2015, 12.4.4 Clock synchronization
Implementation guidance for cloud service provider	The cloud service provider should provide information to the cloud service customer regarding the clock used by the cloud service providers logged putting infrastructure components in Service customer can synchronize local clocks with the cloud clock.
Additional technical information	VM time synchronization with the cloud computing environment is required for cloud service customers in IaaS. Generally VM time synchronization methods are as follows: — NTP (Network Time Protocol) method — Hypervisor method

Control		ISO/IEC 27017:2015, 12.4.4 Clock synchronization	
1	Security implementation standard	The cloud service provider uses either NTP or Hypervisor method to provide the means for synchronizing VM time.	
	Technical note on security implementation standard	The cloud service customers need to set up time synchronization of their own VMs based on the method provided.	
	1.1	Practice guide	Check if the cloud service provider provides a method for time synchronization.
		Evidence assumed	Result of checking if NTP server is provided and cloud service customers have an access to the server via NTP protocol. Result of checking if Hypervisor provides time synchronization and cloud service customers can use the function to synchronize time.
		Method	Test

Control		ISO/IEC 27017:2015, CLD.12.4.5 Monitoring of cloud services	
Implementation guidance for cloud service provider		The cloud service provider should provide capabilities that enable the cloud service customer to monitor specified aspects, relevant to the cloud service customer, of the operation of the cloud services. For example, to monitor and detect if the cloud services is being used as a platform to attack others or if sensitive data is being leaked from the cloud services. Appropriate access controls should secure the use of the monitoring capabilities. The capabilities should provide access only to information about the cloud service customer's own cloud service instances. The cloud service provider should provide documentation of the service monitoring capabilities to the cloud service customer. Monitoring should provide data consistent with the event logs described in 12.4.1 and assist with SLA terms.	
Additional technical information		In general, as defining nefarious use of cloud services is difficult, network traffic which exceeds a certain amount and storage access as such will be detected.	
1	Security implementation standard	Use a logging or monitoring function to detect the occurrence of status defined as nefarious use of cloud services.	
	Technical note on security implementation standard	See 12.4.1.	
	1.1	Practice guide	Check if the monitoring system is defined so that an event defined as nefarious use of cloud services will be detected.
		Evidence assumed	Definition of the monitoring system parameters
		Method	Examine/Observe

Control		ISO/IEC 27017:2015, 12.6.1 Management of technical vulnerabilities
Implementation guidance for cloud service provider		The cloud service provider should make available to the cloud service customer information about the management of technical vulnerabilities as it applies to the cloud services and the information systems it uses.
Additional technical information		Technical vulnerabilities depend on the software version. In general, as cloud computing infrastructure components use more than one version from the same software, it is required to determine if the vulnerabilities exist in computing resources in use.
1	Security implementation standard	When technical vulnerabilities are found in cloud computing infrastructure components, identify cloud service customers who are using the computing resources with the vulnerabilities and provide them with information on those vulnerabilities. See the description in "12.1.2 Change management" for searching for the relationship of computing resources with cloud service customers.

Control		ISO/IEC 27017:2015, 12.6.1 Management of technical vulnerabilities	
	Technical note on security implementation standard	See the description in "12.1.2 Change management" for searching for the relationship of computing resources with cloud service customers.	
	1.1	Practice guide	Check if service customers who are using the computing resources with the vulnerabilities found are identified and provided with information on technical vulnerabilities.
		Evidence assumed	Notification mail on technical vulnerabilities and Portal screen, etc.
		Method	Examine/Observe

C.6 Server virtualization

C.6.1 Overview of server virtualization

Server virtualization abstracts a physical server (consisting of a CPU, memory, and I/O devices, etc.) to a logical resource. Generally, the server virtualization is structured as shown in Figure C.3.

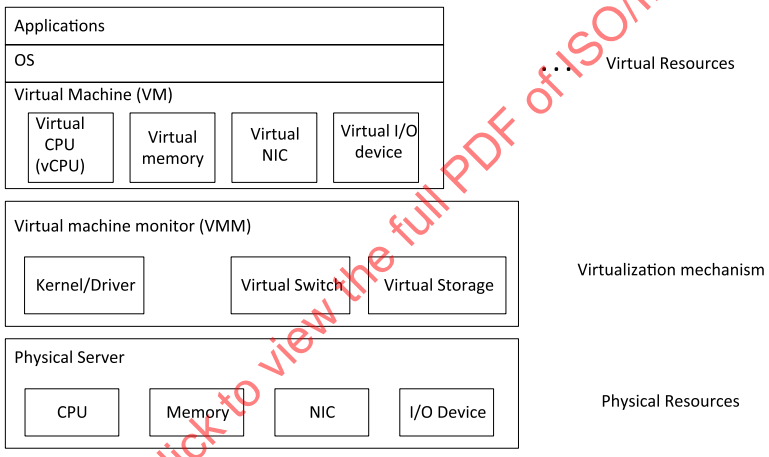

Figure C.3 — Overview of server virtualization

a) **CPU virtualization** allocates customer VMs to the physical CPU on the Virtual Machine Monitor (VMM) on a physical server as virtualization resources on a virtual "core" basis.

CPU virtualization enables to oversubscribe or allocate more virtual CPUs than the number of physical CPU cores for the entire server.

At over-subscription, VMM performs CPU scheduling and such processing as switchover of virtual CPUs allocated to physical CPU cores. Therefore, note that simultaneous heavy processing by more than one VM increases the contention rate of the physical CPUs, consuming CPU resources for the CPU scheduling as well as latency before the CPU resources are allocated, which can affect processing performance.

b) **Memory virtualization** allocates virtual machine's memories on the physical server memories. Similar to the CPU virtualization, virtualizing the memory allows over-subscription, meaning that the total memory size seen from the virtual machine is larger than the actual memory size on the physical server. Memory over-subscription includes a method in which memories are allocated dynamically to a VM (ballooning) and another method in which more than one VM can share the identical memory. In both methods, the sum of the minimum values of the memory allocated to each VM should be smaller than the size of the memory equipped with the physical server.

c) **Storage virtualization**: The storage of a virtual machine is handled as a file set on the storage of a physical server. However, the problem is an occupied band and storage speed, etc., at the

transmission of large amount of data when migrating a virtualized server between physical servers. Therefore, generally, the system which provides cloud service is often designed so that access is via the SAN (storage area network) by installing a common storage server.

d) **I/O virtualization** virtualizes a series of peripherals, including a NIC, HBA, and serial port adapter. Virtualized adapter port is used by connecting to a virtual machine, which is set to work on VMM with VMM settings, or by connecting to a physical adapter port on the physical server. Note that I/O function of the HBA and NIC are highly shared hardware compared to memories and CPUs and often becomes a bottleneck particularly in the function for virtualization.

C.6.2 Application of server virtualization in the cloud services

a) Tenant separation in the server virtualization

In the general virtualized environment design, virtualized servers are designed as completely independent resources and connected via a virtual network between VMs.

Therefore, the minimum network security measures are required for separating VM resources. In addition, what specially should note on the virtualization environment is to correct the vulnerability of the virtualization environment itself provided by a legitimate source.

Furthermore, a special virtualization environment provides a fast communication route between VMs for mutual connection or enables data exchange between VMs via a physical port of the physical server. Therefore, attention should be paid to other I/Os than NIC.

To protect virtual resources, a technology by which memories and IOs are accessed on VMM or a privileged VM exists. Using this technology, the behaviour on the VM can be monitored and an invalid program operation can be detected to protect the resources. However, remember not to install this technology carelessly even though an access from VMM or the privileged VM is useful for the security of virtual resources, because this can provide an attack route to bad users.

b) Ensured availability in the server virtualization

Live migration is a function that migrates the VM operation environment onto a different physical server without deactivating the VM. Live migration is implemented by starting up a VM image stored on a shared storage on the VMM of the destination physical server, transferring data on cache memory via LAN, as well as succeeding the virtualized I/O. This mechanism allows the memory content to flow on LAN at the live migration, and memory data security and LAN security are critical. In the live migration, the administrator migrates the VM between physical servers, or a high-availability technology is provided, by which the VM can be migrated between physical servers automatically when a failure occurs in the environment.

If a failure is detected by monitoring with this kind of high-availability technology, provided services will be suspended for a certain period of time because the image of the virtual machine working on the faulty physical server is activated on another physical server working normally. A failure-resistant virtualization environment is also provided as a technology to reduce the time of service suspensions which occur in the high-availability technology. The failure-resistant virtualization environment includes implementation that operates the primary and secondary VMs on more than one physical server and synchronizes both VMs each other at all times. Under normal operation, the primary VM provides the service and the secondary VM can take it over the moment a failure occurred to provide the failure resistance. Note that both technologies require available resources on another physical server, not on the same physical server.

c) Capacity administration in the server virtualization

Virtualized memories or CPU resources can be allocated dynamically during operation by using an appropriate OS. Because up to the resources on the physical server can be allocated, free space can need to be assured by using the above live migration technology to migrate the VM to another physical server, considering the resources used by other VMs. Physical server resources are indexed by:

— number of CPU cores;

— memory size;

— disk I/O performance;

— disk size;

— network I/O performance.

The total required resources can be calculated by multiplying the total of these indexes provided as services for a simple virtualized environment by overhead loaded for the virtualization. When service availability is considered, a margin should be assured per physical server, as well as resources.

The focus of the indexes, and the way services are provided, depends on the business model or SLA of the cloud service provider. In any case, it is critical that resources currently provided and available resources should be monitored to continue to provide hardware resource. This kind of monitoring is performed mainly at the Service management for integrity of the entire cloud services environment. However, note that a resource usage monitoring tool can be installed on the VMM or privileged VM on the server virtualization.

C.6.3 Carrying out the technical assessment for the server virtualization

C.6.3.1 Access Control

For the segregation in server virtualization, see C.6.2 a).

Control		**ISO/IEC 27017:2015, CLD.9.5.1 Segregation in virtual computing environments**	
Implementation guidance for cloud service provider		The cloud service provider should enforce appropriate logical segregation of cloud service customer data, virtualized applications, operating systems, storage, and network for: — the separation of resources used by cloud service customers in multi-tenant environments; — the separation of the cloud service provider's internal administration from resources used by cloud service customers. Where the cloud service involves multi-tenancy, the cloud service provider should implement information security controls to ensure appropriate isolation of resources used by different tenants. The cloud service provider should consider the risks associated with running cloud service customer-supplied software within the cloud services offered by the cloud service provider.	
Additional technical information		Implementation of the logical separation depends on the technologies applied to the virtualization	
1	Security implementation standard	Separation of cloud service customers in multi-tenant environments.	
	Technical note on security implementation standard	There is a communication path between VMs using memory and virtual ports, which may become a communication path between “virtual resources”.	
	1.1	Practice guide	Make inactive functions accessed directly between VMs
		Evidence assumed	Confirm that functions accessed directly between VMs within VMM are made inactive
		Method	Examine/Observe, Examine /Review
2	Security implementation standard	Separation of the cloud service provider’s internal administration from the cloud service customers’ virtual environments.	

Control		ISO/IEC 27017:2015, CLD.9.5.1 Segregation in virtual computing environments	
	Technical note on security implementation standard	Within VM-VMM separation, VM-VM management is active in the same way as noted in previous section. In addition, as communication path may be created with tools implemented from security or availability aspect in VM-VMM, vulnerabilities in those tools may prove to be a loophole in VM-VMM configuration.	
	2.1	Practice guide	Applying segregation functions of virtualization software Enable the partition function on virtualization environment.
		Evidence assumed	Confirmation of Access Control Policy in VMM Confirm that Transparent Page Sharing is inactive in VMM
		Method	Examine/Observe, Examine/Review
	2.2	Practice guide	Physical segregation of a cluster of virtual systems
		Evidence assumed	Confirm that Virtualization support function in physical server is active
		Method	Examine/Observe, Examine/Review
3	Security implementation standard	Perform vulnerability management	
	Technical note on security implementation standard	Products built with security measures (Common Criteria qualified, etc.) should be used in virtualization platform (host OS, Hypervisor, etc.)	
	3.1	Practice guide	Confirm that products used in virtualization platforms are built with security measures in mind.
		Evidence assumed	Base design document for virtualization platform
		Method	Examine/Review
	3.2	Practice guide	Sharing of vulnerability information within operations
		Evidence assumed	Confirmation of status of vulnerability information sharing (Check posted information on portal page, etc.)
		Method	Examine/Observe

Control		ISO/IEC 27017:2015, CLD.9.5.2 Virtual Machine Hardening	
Implementation guidance for cloud service provider		When configuring virtual machines, cloud service customers and cloud service providers should ensure that appropriate aspects are hardened (e.g. only those ports, protocols and services that are needed to run the cloud services are enabled) and the appropriate technical measures are in place (e.g. anti-malware, logging) for each virtual machine used.	
Additional technical information		The VM/VMM and physical server achieve not only by the VM operating system, but virtual machine hardening also. As these are all closely related, virtual machine hardening requires cooperation from the cloud service customer and cloud service provider.	
1	Security implementation standard	When configuring virtual machines, only necessary device and/or service remain in effect.	
	Technical note on security implementation standard	Regarding the Virtual Machine Hardening, this control does not explain anew about enhancing a virtualized server because general server enhancing technologies can be applied to it. However, there is a technology providing security for a server from a VMM. If this technology is used, its review method should also comply with the method defined in ISO/IEC 27002.	
	1.1	Practice guide	Confirm that provided VM functionality within VMM is configured as the bare minimum.
		Evidence assumed	Result of confirmation
		Method	Examine/Observe, Examine /Review