TECHNICAL REPORT

ISO/IEC TR 27008

First edition
2011-10-15

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

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

Reference number
ISO/IEC TR 27008:2011(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

Introduction

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

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

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

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

1 Scope

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

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

2 Normative references

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

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

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

3.1
review object
specific item being reviewed

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

3.3
security implementation standard
document specifying authorized ways for realizing security

4 Structure of this Technical Report

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

Background information is provided in Clause 5.

Clause 6 provides an overview of information security control reviews.

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

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

5 Background

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

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

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

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

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

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

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

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

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

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

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

6 Overview of information security control reviews

6.1 Review process

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

Preliminary information can come from a variety of sources:

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

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

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

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

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

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

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

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

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

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

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

Audit managers should dispassionately review evidence to check that:

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

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

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

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

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

6.2 Resourcing

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

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

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

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

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

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

7 Review methods

7.1 Overview

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

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

- examine,
- interview, and
- test.

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

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

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

7.2 Review method: Examine

7.2.1 General

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

Review objects typically include:

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

Typical information security control review auditor actions may include:

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

7.2.2 Attributes

7.2.2.1 Generalized examination

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

7.2.2.2 Focused examination

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

7.2.2.3 Detailed examination

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

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

7.2.2.4 Representative examination

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

7.2.2.5 Specific examination

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

7.2.2.6 Comprehensive examination

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

7.3 Review method: Interview

7.3.1 General

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

Review objects typically include individuals or groups of individuals.

Typical information security control review auditor actions may include interviewing:

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

7.3.2 Attributes

7.3.2.1 Generalized interview

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

a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors.

7.3.2.2 Focused interview

In addition to the requisites of the generalized interview the focused interview includes in depth discussions in specific areas with individuals, or groups of individuals. This type of interview additionally employs in depth questions in specific areas where responses indicate a need for more in depth investigation. Focused interviews provide a level of understanding of the control necessary for determining whether the control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.

7.3.2.3 Detailed interview

In addition to the requisites of the focused interview the detailed interview includes more in depth, probing questions in specific areas where responses indicate a need for more in depth investigation or where called for by review procedures. Detailed interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

7.3.3 Coverage attribute

The coverage attribute addresses the scope or breadth of the interview process and includes the types of individuals to be interviewed (by organizational role and associated responsibility), the number of individuals to be interviewed (by type), and specific individuals to be interviewed.

7.3.3.1 Representative interview

Interview that uses a representative sample of individuals in key organizational roles to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.

7.3.3.2 Specific interview

Interview that uses a representative sample of individuals in key organizational roles and other specific individuals deemed particularly important to achieving the review objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.

7.3.3.3 Comprehensive interview

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

7.4 Review method: Test

7.4.1 General

The process of exercising 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 and possible effects on the operation of the organization have to be considered and approved by management before commencing the testing, also considering the options of running tests outside operational 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 may lead both to financial consequences and impact the reputation of the organization so particular care has to be taken into the test planning and its correct contractualization (including consideration of legal aspects).

False positives and false negatives results of the tests have to be carefully investigated by the information security control review auditor before making any induction.

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

Typical information security control review auditor actions may include:

- testing access control, identification, authentication and review mechanisms,
- testing security configuration settings,
- testing physical access control devices,
- 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, and
- verifying the cascade resilience of security measures.

Note: Attributes do not apply for testing

7.4.2 Test types

7.4.2.1 Blind Testing

The information security control review auditor engages 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 control review auditor. The breadth and depth of a blind review can only be as vast as the information security control review auditor's applicable knowledge and efficiency allows. Thus this testing is of limited use in security reviews and should be avoided. This is also commonly referred to as Ethical Hacking.

7.4.2.2 Double Blind Testing

The information security control review auditor engages 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 of agitation.

7.4.2.3 Gray Box Testing

The information security control review auditor engages 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 gray box review tests the skills of the information security control review auditor. The nature of the test is efficiency. The breadth and depth depends upon the quality of the information provided to the information security control review auditor before the test as well as the information security control review auditor's applicable knowledge. Thus this testing is of limited use in security reviews and should be avoided. This type of test is often referred to as a Vulnerability Test and is most often initiated by the target as a self-assessment activity.

7.4.2.4 Double Gray Box Testing

The information security control review auditor engages 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 gray box review tests the target's preparedness to unknown variables of agitation. The breadth and depth depends upon the quality of the information provided to the information security control review auditor and the review object before the test as well as the information security control review auditor's applicable knowledge.

7.4.2.5 Tandem Testing

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

7.4.2.6 Reversal

The information security control review auditor engages 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 control review 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 upon the quality of the information provided to the information security control review auditor and the information security control review auditor's applicable knowledge and creativity. This is often also called a Red Team exercise.

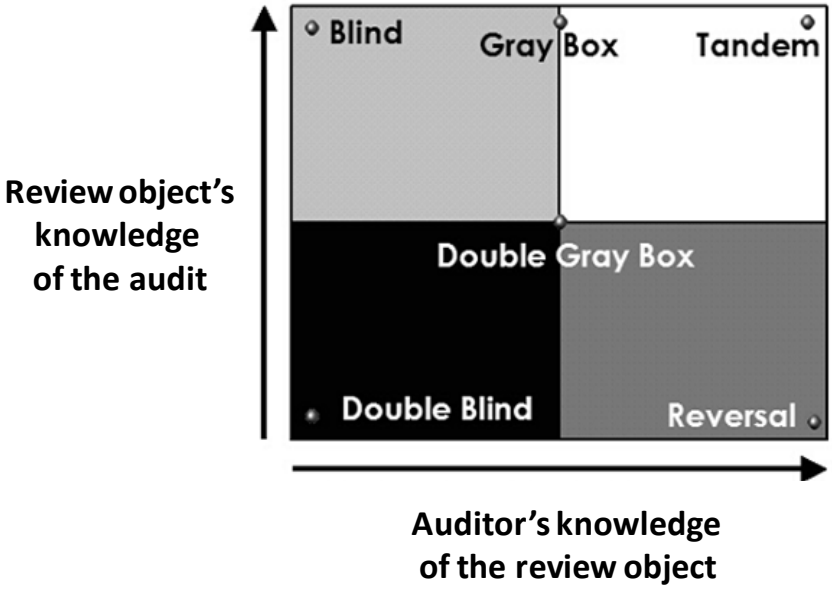

Figure 1 – Test types

7.4.3 Extended review procedures

In addition to the review procedures that are applied to individual controls, an extended review procedure can be applied to the review as a whole. The extended review procedure is designed to work with and complement the review procedures to contribute to the grounds for confidence in the effectiveness of the controls.

The extended review procedure and the associated review objectives are also closely linked to the risk level of the information system.

8 Activities

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 control review 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 preparatory/implementation stage),
- ensuring that selected 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 being 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 having an interest 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 control review auditor or audit team that will be responsible for conducting the review, considering issues of information security control review auditor independence,
- collecting artefacts to provide to the information security control review auditors (e.g., information security controls documentation including organizational charts, policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements, previous review results), and
- establishing a mechanism between the organization and the information security control review auditors to minimize ambiguities or misunderstandings about control implementation or control weaknesses/deficiencies identified during the review.

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

- obtaining a general understanding of the 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,
- obtaining an understanding of the structure of the information assets (i.e., system architecture),
- obtaining a thorough understanding of all 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., policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements),
- obtaining previous review results that may 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 control review 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 information security control review auditor also needs access to

the security policies for the information system and any associated implementing procedures, any materials (e.g., security plans, records, schedules, review reports, after-action reports, agreements, accreditation packages) associated with the implementation and operation of controls, and the objects to be reviewed.

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 Developing a plan

8.2.1 Overview

Information security control review 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 upon the purpose/scope of the review. Information security control review auditors should estimate and reduce the risk and impact (where possible) of the review on the normal operation of the organization and select the appropriate review procedures to be used during 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 control review auditors should tailor the selected review procedures for the information system risk level and the organization's actual operating environment. They should also develop additional review procedures, if necessary, to address security controls, control enhancements and additional assurance needs that are not covered in this document.

The plan should be designed to include the phase for determining 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 include 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. Information security control review auditors should thereafter finalize the review plan and obtain the necessary approvals to execute the plan.

8.2.2 Scope

The 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 control review 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. The selection of controls depends on the continuous monitoring schedule established, items on the plan of action and adequate milestones. Controls with greater volatility should be reviewed more frequently.

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 to 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 compliance checking 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 control review 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 most effectively make appropriate determinations and to satisfy review objectives,
- selecting the review method depth and coverage attribute values necessary to meet the review expectations based upon 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 successfully carry out the review,
- 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 external providers, 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 may 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 termed 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 control review 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 control review auditors should select only those methods and objects that most effectively contribute to making the determinations associated with the review objective. The 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. It will not be necessary, in most cases, to apply every review method to every review object to obtain the desired review results. And for specific reviews and comprehensive reviews, it may be appropriate to employ a method not currently listed in the set of potential methods or to not employ a method that is listed.

8.2.5 Previous findings

8.2.5.1 Overview

Information security control review 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 control review auditor should determine the

- credibility of the evidence,
- appropriateness of previous analysis, and
- applicability of the evidence to current information asset conditions.

It may 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 employed by the organization in an information system, then the information security control review auditor may need to supplement the original test results with additional testing to cover that configuration setting for the current information system environment.

The following sections 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 may have become ineffective due to changing conditions relating to the information asset or the surrounding environment. Thus, review results that were found to be previously acceptable may no longer provide credible evidence for determination of control effectiveness, and a new review would be 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 may 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 may include the findings from a previous security review as long as:

- it is expressly permitted in the audit plan,
- information security control review 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 audit findings are clearly stated in the audit 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 operates is more likely to change with the passage of time, possibly invalidating the original conditions or assumptions on which the previous review was based.

8.2.6 Work assignments

Information security control review 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 no information security control review auditor independence was 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, alternative review approaches may need to be applied. This may result in the need to tailor the review procedures described in Annex A. Where required assurances of agreed-upon controls for an information system are documented in contracts or service-level agreements. The information security control review 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 control review 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 upon with regard to protecting the information assets under review. Applicable information from these reviews, if deemed reliable, should be incorporated into the report.

8.2.8 Information assets and organization

Review procedures may be adapted to address system/platform-specific or organization-specific dependencies. This situation arises frequently in the review procedures associated with the security controls from the technical information security controls (i.e., access control, audit and accountability, identification and

authentication, system and communications protection). Recent test results may 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 may 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. E.g. 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 in Section 7.5 is applied on a review-by-review basis typically 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 control review auditors can have a certain degree of flexibility in organizing a review plan that meets the needs of the organization. Therefore this presents 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 control review 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 control review auditors may wish to consolidate interviews with key organizational officials dealing with a variety of information security-related topics. Information security control review auditors may 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 could 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 may provide information that facilitates understanding and review of other controls. For example, controls areas may produce general descriptions of the information assets. Reviewing these security controls early in the review process may 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 may 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 might 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 Conducting reviews

After the review plan is approved by the organization, the information security control review auditor executes the plan in accordance with the agreed-upon 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 executed by an information security control review auditor produces one the following findings

- satisfied (S),
- partly satisfied (P), or
- other than satisfied (O).

A finding of satisfied indicates 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. A finding of partly satisfied indicated 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 the control will reach a satisfied result (S). A finding of other than satisfied indicates 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 may need to be addressed by the organization. A finding of other than satisfied may also indicate that for reasons specified in the review report, the information security control review auditor was unable to obtain sufficient information to make the particular determination called for in the determination statement.

The information security control review auditor findings (i.e., the determinations made) should be an unbiased, factual reporting of what was found concerning the control reviewed. For each finding of other than satisfied, information security control review auditors should indicate which parts of the security control are affected by the finding (i.e., those 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 control review auditor should also note the potential for compromises to confidentiality, integrity, and availability due to other than satisfied findings. If the review reveals major non-conformities (i.e. “other than satisfied” findings which deviate significantly from the planned status), which might carry a significantly increased risk for the organization, the information security control review auditor should immediately inform the person responsible for this control and management such 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 control review auditor (in the form of review findings) necessary to determine the effectiveness of the controls employed and the organization's overall effectiveness in implementing selected and appropriate controls based upon the information security control review 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 etcetera.

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 etcetera).

The information system owner relies on the information security expertise and the technical judgment of the information security control review 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 control review auditor (i.e., findings of satisfied or other than 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 may choose to act on selected information security control review 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 control review auditor should review controls, which are modified, enhanced, or added during this process again prior to producing of 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 control review 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 of satisfied and other than satisfied, 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 may decide that certain review findings marked as other than satisfied are of an inconsequential nature and present no significant risk to the organization. Alternatively, the asset owner and managers may decide that certain findings marked as other than satisfied are significant, requiring immediate remediation actions. In all cases, the organization reviews each information security control review auditor finding of other than satisfied and applies its judgment with regard to the severity or seriousness of the finding (i.e., the potential adverse affect on the organization's operations and assets, individuals, other organizations *etc.*), and whether the finding is significant enough to be worthy of further investigation or remedial action. Senior management involvement in the mitigation process may be necessary in order to ensure that the organization's resources are effectively allocated in accordance with organizational priorities, providing resources first to the information assets that are supporting the most business critical processes for the organization or 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 typically performed. This includes verifying the validity of implemented solutions to previous findings. Organizations may also choose to conduct follow-up activities at the next review, especially for those issues that are non-critical or urgent.

Annex A
(Informative)

Technical compliance checking practice guide

This Annex provides a set of practical guides for technical compliance checking by using typical technical controls depicted from ISO/IEC 27002. Each control in this Annex A is basically organized by the following structure of statements and guidance.

"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

   1.3

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

   2.3

Each technical control has additional technical information to give further support to information security control review 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 supplemental "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 may differ among organizations. However, the names used in this Annex can be considered as generally accepted in the field of technical compliance checking. "Method" provides an appropriate approach to technical compliance checking in accordance with the practice guide above.

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

A.1 Technical checking of the control against malicious code.	
Control	**ISO/IEC 27002 10.4.1 Controls against malicious code** Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.
Additional technical information	Malicious code (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 control review 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 control review 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 control review auditors should ensure that the detection/prevention system works appropriately under each circumstance. Note Information security control review 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 malicious code 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, for malicious code before use; 2) checking electronic mail attachments and downloads for malicious code before use; this check should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization; 3) checking web pages for malicious code.	
	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	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 control review auditors check that the detection/prevention system is placed comprehensively and effectively by reviewing the system specification or network diagrams. 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, desk top 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 control review 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 control review 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 use for reviewing or browsing web pages, information security control review 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 control review auditors note that it is also placed in the web servers inherently in the system specification without clear description.
		Evidence assumed	System specification, Network diagram
		Method	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 malicious code 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 malicious code and repair system is managed into an integrated system. 2) Check that detection of malicious code and repair system is placed, and it is working appropriately for detecting any electronic mail attachments and downloads at electronic mail servers, sampled desk top 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 malicious code in the html mail. 3) Check that detection of malicious code 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 use 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 malicious code in the web services such as apache, IIS, etc.
		Evidence assumed	Facilities of detection of malicious code and repair system is placed, for example: ・ File server; ・ E-mail server; ・ Sampled desktop PCs; ・ Mobile computers; ・ an exclusive d detection of malicious code 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).
		Method	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. 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 shows that the function has been running. Rather most of the browser shows the message when unauthorized scripts are detected.
		Evidence assumed	・ The detection system in service ・ Log files output from detection system ・ Records of detection system alert ・ Message from detection system in web browser
		Method	Examine/Observe
2	Security implementation standard	Malicious code 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	Practice Guide	Check the design of Malicious code 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 Malicious code 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

A.2 Technical checking of the control on audit logging.	
Control	**ISO/IEC 27002 10.10.1 Audit logging** Audit log recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
Additional technical information	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 analyze 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 equipments, which produce the logs, should have been tuned up or some rules are applied to them.

<table>
<tr><td colspan="2"></td><td colspan="2">The method of logging depends on system structure, architecture and implemented applications.

Information security control review 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.</td></tr>
<tr><td rowspan="3">1</td><td>Security implementation standard</td><td colspan="2">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.</td></tr>
<tr><td>Technical note on security implementation standard</td><td colspan="2">In order to find out the security events and their causes, information security control review auditors check and analyze the status of system operation, use and change from the record in the log. In order to investigate the events, causality of incidents, audit logs from multiples systems need to be combined. For this purpose, to understand the location and type of audit log files from consideration of system structure/architecture/configuration are important.</td></tr>
<tr><td>1.1</td><td>Practice Guide</td><td>Check that system design of logging is based on Security implementation standard.</td></tr>
</table>

		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/ Observe
	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 control review 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	Check the integrity of the records in the audit logs to determine the logging is appropriate. Note: Some records should have been recorded in the audit logs are missing due to the lack of performance, capability of the system, or some other reasons, even though the setting of logging is appropriate.
		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 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.	
	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/Observe
	2.2	Practice	Check the setting of the storing period of audit logs in the system are

		Guide	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/Observe
	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/Observe

A.3 Technical checking of the control on privilege management.		
Control		**ISO/IEC 27002 11.2.2 Privilege management** The allocation and use of privileges 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 control review 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.

	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 that is 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 the regular ID if the operation no needs 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
	2.2	Practice Guide	Check that the privilege 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 control review auditors should try interview to check the privilege uses a different user ID for normal business use when the log indicates that privilege uses only privilege ID.
		Evidence assumed	・Log file ・System configuration of login by 'root'.
		Method	Examine/Observe

A.4 Technical checking of the control on Back-up.	
Control	**ISO/IEC 27002 10.5.1 Information back-up** Back-up copies of information and software should be taken and tested regularly in accordance with the agreed back-up policy.
Additional technical information on the Control	To take back-up appropriately, organization standard should be defined in accordance with back-up policy and it should be reflected to back-up design document. Back-ups 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 back-up, adequate back-up site, back-up path and back-up method should be selected in accordance with the organization's back-up policy. In terms of back-up site, the organization should select whether onsite or offsite as a back-up site. Onsite back up is considered to be much faster as compared to offsite back up to take back-up and restore. Offsite back up is often selected in order to prevent from the influence of local disasters such as fires, floods, or earthquakes. In terms of back-up path, whether online or offline should be selected. Online back up means that data is backed up via network or communication line. Offline back up means that backed-up data is physically transported with removable media such as DLTs or CD/DVDs. Back-up method is classified several options such as full back up, incremental back up and differential back up. Full back up means back up 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 back up means to take back up 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 back up means to take back up the data that have changed since the last full backup. It will need less time and data capacity than full back up and more simple and easier method to restore than incremental back up.

1	Security implementation standard	The extent (e.g. full or differential back-up) and frequency of back-ups 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 back-up/restore time and data capacity for back-ups. Assessors should assess that the adequate back-up 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 back-up design is based on security implementation standard.
		Evidence assumed	・Back-up specification document ・Business and security requirements definition document ・Back-up design document
		Method	Examine/Review
	1.2	Practice Guide	Check that setting of system configuration files for back up is as described in back-up design document.
		Evidence assumed	・Back-up design document ・Back-up system configuration files
		Method	Examine/Review
	1.3	Practice Guide	Check that back up has been taken as documented in back-up design document.
		Evidence assumed	・Back-up design document ・Log files ・Back-up media
		Method	Examine/Observe
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 back-up 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

A.5 Technical checking of the control on the Network security management.			
Control		**ISO/IEC 27002 10.6.2 Security of network services** Security features, service levels, and management requirements of all network service should be identified and included in any network services agreement, 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, assessors 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	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	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
	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	・Log files ・Alert message ・Network service design document
		Method	Examine/Observe

A.6 Technical checking of the control on the User responsibilities.	
Control	**ISO/IEC 27002 11.3.1 Password use** Users should be required to follow good security practices in the selection and use of passwords.
Additional technical information on the Control	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. Assessors should assess that the authorization functions with passwords are placed at the computer resources effectively, and those functions work appropriately.

1	Security implementation standard	Select quality passwords with sufficient minimum length which are: 1) easy to remember; 2) not based on anything somebody else could 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.	
	Technical note on Security implementation standard	The passwords that are easy to remember for another user are vulnerable in general.	
	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) 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

Annex B
(Informative)

Initial information gathering (other than IT)

The lead information security control review auditor should allocate a information security control review auditor with the relevant competence and experience for each information security field.

Initial questions to relevant staff may include areas and non-exhaustive list of examples indicated below.

B.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?

B.2 Policies

a. Hierarchy:

   i. Are the information security policies derived from the business objectives and from the overall security policy?

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

b. Comprehensive:

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

   ii. Are the policies complete in their design encompassing strategy, tactics, and operations?

c. Formulation:

   i. Are the policies a 'copy-paste' of ISO 27002, or are the control objectives and controls tailored to the specific context?

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

   iii. An action expected within a policy or a procedure should consider the 'fundamental' questions: Who, When, Why, What, Where, How

      - if the person responsible (who) to perform the action is not defined, who will achieve the set objectives?
      - If the target time (when) for performing the action is not defined, will it be started or finished in due time?
      - If the aim or objective of an action is not defined (why), will the action be correctly understood and its importance adequately considered?

- If the action itself (what) is not defined, how will it be possible to perform it?
- 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)?
- If an action in a procedure doesn't clearly define how things have to be done, how could it correctly performed (how)?
- If an action doesn't also define the indicators and controls aimed at verifying it correctly evolves and achieves its objectives, how could an organization make sure the objectives are, or can be, achieved?

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

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

- unspecific objectives are not easy to clearly recognize and the person(s) responsible to achieve it is generally not defined
- if the objective is not measurable, there is little chance that an organization will be able to verify if it is achieved or not
- 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'
- 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
- 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.

B.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?

B.4 Physical and environmental security

B.4.1 Are the sites safe for information?

a. 'Zones'

i. Are areas accessible to the public sufficiently isolated from business areas?

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

iii. Are these 'secured zones' appropriately segregated to avoid information exchange?

b. Locations

i. Are the different zones clearly identified and appropriately situated?

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

iii. Are the locations appropriately labelled and the critical ones out of sight of 'externals'?

c. 'Gates' – access points
    i. Do doors and windows and 'openings' in the borders provide the same protection as the 'borders' when they are closed?
    ii. Is an appropriate access control in place to enter and exit the 'locations'
    iii. Is there an anti-intrusion system?
    iv. Are there 'emergency exits' allowing for enough mobility of information, people and equipment?
d. Corridors and 'paths'
    i. Are 'paths' to the zones and locations identified
        - Paths for people
        - Cables (paths for information)
    ii. Are there alternative paths?
    iii. Are these 'paths' protected and monitored?
e. Monitoring
    i. Can the monitoring resources see without being seen?
    ii. Can the monitoring resources see an intrusion coming from far?
    iii. When is monitoring active?
    iv. Where and how are records kept and analyzed?
f. Furniture
    i. Appropriate for information storage?
    ii. Correctly located?
    iii. Operating as expected?

B.4.2 Are the sites safe for ICT? (Environmental aspects)

a. Power provision
    i. Enough/Appropriate
    ii. Alternate?
b. Air conditioning provision
    i. Enough/Appropriate
    ii. Alternate?
c. Fire fighting provision
    i. Enough/Appropriate
    ii. Alternate?

B.4.3 Are the sites safe for People?

a. Do emergency exists exist (and with appropriate controls)
b. Are 'leakages' (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 can't be injured?
e. Are the 'gates' installed and operated so that people can't be injured?
f. Is furniture installed and maintained so that people can't be injured?

B.5 Incident management

a. Are information security incidents defined?

b. Is there a capability build to respond to information security incidents:

   i. Guidelines?

   ii. Roles and responsibilities?

   iii. Means & resources?

Bibliography

[1] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[2] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

[3] ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

[4] ISO/IEC 27006:2007, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[5] ISO/IEC 27007:2011, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[6] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

[7] ISO Guide 73:2009, *Risk management — Vocabulary*

[8] NIST Special publication (SP) 800-53A, *Guide for reviewing the controls in federal information systems*, July 2008. Available from: http://csrc.nist.gov/publications/PubsSPs.html

[9] Institute For Security And Open Methodologies, *Open-Source Security Testing Methodology Manual*. Available from: http://www.isecom.org/osstmm/

[10] Federal Office for Information Security (BSI), Germany, Standard 100-1, *Information Security Management Systems (ISMS); 100-2, IT-Grundschutz Methodology; 100-3, Risk Analysis based on IT-Grundschutz and IT-Grundschutz Catalogues* (available in German and English). Available from: https://www.bsi.bund.de/cln_174/EN/Publications/publications_node.html

[11] Information Security Forum, *The Standard of Good Practice for Information Security*, 2007. Available from: https://www.securityforum.org/services/publicresearch/

ICS 35.040
Price based on 36 pages