| **Final Committee Draft**<br>**ISO/IEC FCD 27006** | |
|---|---|
| Date:<br>**2006-05-18** | Reference number:<br>ISO/IEC JTC 1/SC 27 **N5098** |
| Supersedes document SC27 N4972rev2 | |
| THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES. | |
| ISO/IEC JTC 1/SC27<br>Information technology - Security techniques<br>Secretariat:<br>Germany (DIN) | Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by:<br>**2006-09-18**<br>Please return all votes and comments in electronic form directly to the SC 27 Secretariat by the due date indicated. |

**ISO/IEC FCD 27006**

Title: Information technology – Security techniques – Requirements for the accreditation of bodies providing certification of information security management systems

Project: 27006

**Explanatory Report**

| **Status** | **SC27 Decision** | **Reference documents** | |
|---|---|---|---|
| | | **Input** | **Output** |
| National Body New Work Item Proposal (N4933) | | Background information presented in N4934 (with Att. 1 = EA-7/03) | Summary of voting on NP 27006 (1.27.53) presented in N5011 |
| Concurrent review of discussion draft presented in N4972 (revised version of EA-7/03, March 2006) | Regional Consultation Meetings (Berlin, Montreal, Singapore) 23/24 March 2006 | Background on ISMS 27001 Certification – **Revision of EA-7/03** (N4971rev1) | Revised draft N4972rev1<br>Summary of Minutes of the Regional Meetings presented in N5009 |
| | Joint EA-7/03 Task Force Meeting in Frankfurt on 2 May 2006 | National Body Comments (see in N5099) | Revised draft N4972rev2 |
| | Joint EA-7/03 Task Force Meeting in Madrid during the 32nd WG1 Meeting on 8th May 2006 | | Revised draft of N4972rev2 |
| | SC27/WG1 Resolution 8 of the 32nd Meeting in Madrid, 8th -12th May 2006 | | Text for FCD 27006 (N5098) |

**FCD Registration and Consideration**

In accordance with resolution 8 of its 18th Plenary Meeting in Madrid, 16th – 17th May 2006, SC27 endorsed the accelerated approval process for project 1.27.53 (27006). Consequently, document SC27 N5098 has been registered with the ISO Central Secretariat (ITTF) as FCD and is hereby submitted for a four-month FCD letter ballot closing by

**2006-09-18**

Medium: Livelink-server

No. of pages: 1 + 49

Address Reply to:
Secretariat, ISO/IEC JTC 1/SC27 -
DIN Deutsches Institut fuer Normung e.V., Burggrafenstr. 6, 10772 Berlin , Germany
Telephone: + 49 2601-2652; Facsimile: + 49 2601-1723; E-Mail: krystyna.passia@din.de,
http://www.ni.din.de/sc27

**ISO/IEC JTC 1/SC 27 N5098**

Date: 2006-05-18

**ISO/IEC FCD 27006**

ISO/IEC JTC 1/SC 27/WG 1

Secretariat: DIN

# Information technology — Security techniques — Requirements for the accreditation of bodies providing certification of information security management systems

*Technologies de l'information — Techniques de sécurité*

**Warning**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (40) Enquiry
Document language: E

G:\ni\PASSIA\ISO_IEC_JTC1_SC27\PROJECT_admin\NP_27006_Jan2006\O3_00_FCD_27006_May2006\SC27N5098_Text_FCD_27006_May2006\ISO-IEC_27006_(E).doc STD Version 2.2

CONTENTS

# 0. Introduction to this Standard

*ISOIEC 17021 Conformity Assessment – Requirements for bodies providing audit and certification of management systems*[1] is an International Standard which sets out criteria for bodies operating audit and certification of organizations' management systems. If such bodies are to be accredited as complying with ISO/IEC 17021 and want to audit or certify Information Security Management Systems (ISMS), some additional guidance to the Standard ISO/IEC 17021 is necessary and is provided this standard.

One aim of this standard is to more effectively enable accreditation bodies to harmonise their application of the standards against which they are bound to assess certification bodies. Harmonisation is an important step towards mutual recognition of accreditation. This standard will also be useful to certification bodies themselves and to those whose decisions are guided by their certificates. For convenience, the headings from ISO/IEC 17021 are first printed in **bold.** Where guidance for ISMS certification is offered, it is, for ease of reference, identified with the letter "G". The requirements against which conformity is determined are found in ISO/IEC 17021.

This Standard will form the basis of mutual recognition agreements between accreditation bodies, and is considered necessary for the consistent application of ISO/IEC 17021. Members of the IAF Multilateral Agreement (MLA), and applicants for membership in that Agreement, will assess each others' implementation of ISO/IEC 17021. All of this guidance is expected to be adopted by accreditation bodies as part of their general rules of operation.

**This document does not define any requirements for accreditation additional to ISO/IEC 17021. The term "shall" is used throughout this document to indicate those provisions which, reflecting the requirements of ISO/IEC 17021 and/or ISO/IEC 27001, which are mandatory. The term "should" is used to indicate guidance which, although not mandatory, is provided as a recognised means of meeting the requirements. Certification bodies whose systems do not follow the ISMS Guidance in any respect will only be eligible for accreditation if they can demonstrate to the accreditation body that their solutions meet the relevant clause of ISO/IEC 17021 and/or ISO/IEC 27001 and of this document in an equivalent way.**

*Note: Please note that the "shall" statements in this document are for compliance with ISO/IEC 17021 (these requirements are for the purpose of accreditation) and ISO/IEC 27001(these requirements are for the purpose of ISMS certification).*

Behind this Standard lies the principle, that if organizations' management systems are certified to a management system standard, such as ISO 9001:2000 or ISO 14001:2004, or an equivalent standard or

[1] *At the creation of this draft, ISO/IEC 17021 was only available as 2nd DIS – this 2nd DIS has been used as the basis fort his first draft. If changes are made in the development process of ISO/IEC 17021, this document needs to be updated to reflect these changes.*

normative document, those systems should give the organization (internally), its business partners, its clients, its customers, and its markets, confidence that the organization is capable of systematically meeting agreed requirements for any product (i.e. services, software, hardware and processed material) supplied within the field specified on the certificate. Certification bodies should demonstrate that the certificates they issue satisfy this principle. A certification body may seek advice from the accreditation body on any matter which may affect its accreditation. The accreditation body should respond with advice or a decision. IAF and ISO/IEC JTC 1/SC 27 have collaboratively prepared this Standard as guidance on the application of ISO/IEC 17021 in conjunction with ISO/IEC 27001.

***NOTE:***

Throughout this document, the terms “management system” and “system” are used interchangeably. The definition of a management system can be found in ISO 9000:2000. The management system as used in this document is not to be confused with other types of system, such as IT systems.

# 1. Scope

This standard provides guidance for the requirements contained within ISO/IEC 17021 and as relating to ISO/IEC 27001. Specifically this guidance relates to the recognition of requirements that need to be demonstrated in terms of competence and reliability in the provision of an information security management system (ISMS) certification by a third-party.
Note: Certification of a management system is sometimes also called registration, and certification bodies are sometimes called registrars. For ease of understanding, this publication always refers to such bodies as "certification bodies". This should not be understood to be limiting.

The guidance contained within this standard can be considered as providing additional interpretation of the requirements for any body providing ISMS certification.

# 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 17021:2006 Conformity Assessment – Requirements for bodies providing audit and certification of management systems

ISO/IEC 27001:2005 Information Technology – Security Techniques – Information security management systems - Requirements

# 3. Terms and Definitions

The following definitions apply to the ISO 17021 references given in this standard. In addition, the definitions from ISO/IEC 17021 and ISO/IEC 27001 apply:

**3.1** Certificate: A certificate issued by a certification body in accordance with the conditions of its accreditation and bearing an accreditation symbol or statement.

**3.2** Certification body: A third party that assesses and certifies the ISMS of a client organization with respect to published ISMS standards, and any supplementary documentation required under the system.

**3.3** Certification document: Document indicating that a client organization's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system.

**3.4** Mark: A legally registered trade mark or otherwise protected symbol which is issued under the rules of an accreditation body or of a certification body indicating that adequate confidence in the systems operated by a body has been demonstrated or that relevant products or individuals conform to the requirements of a specified standard.

**3.5** Organization: Company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration and is able to ensure that information security is exercised.

# 4. Principles for certification bodies

## 4.1 General

**ISO/IEC 17021 Clause 4.1 states general principles for certification bodies.**

## 4.2 Impartiality

**ISO/IEC 17021 Clause 4.2 states general principles for the impartiality of certification bodies.**

## 4.3 Competence

**ISO/IEC 17021 Clause 4.3 states general principles for the competence of personnel of the certification bodies. This is further detailed in Section 7.1.**

## 4.4 Responsibility

**ISO/IEC 17021 Clause 4.4 states general principles for the responsibilities of the certification bodies and the clients.**

## 4.5 Openness

**ISO/IEC 17021 Clause 4.5 states general principles for openness of the certification bodies.**

## 4.6 Confidentiality

**ISO/IEC 17021 Clause 4.6 states general principles for confidentiality.**

## 4.7 Responsiveness to complaints

**ISO/IEC 17021 Clause 4.7 states general principles for the resolution of complaints.**

# 5. General requirements

## 5.1 Legal and contractual matter

**ISO/IEC 17021 Clause 5.1 states general requirements for legal and contractual matters applying to certification bodies. This clause includes**

**5.1.1 Legal responsibility**

**5.1.2 Certification agreement**

**5.1.3 Responsibility for certification decisions**

## 5.2 Management of impartiality

**ISO/IEC 17021 Clause 5.2 states requirements for how the certification bodies should manage and ensure impartiality.**

***ISMS Specific Guidance***

**G 5.2 Conflicts of interest**

Consultancy is considered to be participation in an active creative manner in the development of the ISMS to be audited by, for example:

a) Preparing or producing manuals, handbooks or procedures;

b) Participating in the decision making process regarding management system matters;

c) Giving specific advice towards the development and implementation of management systems for eventual certification.

Certification bodies can carry out the following duties without them being considered as consultancy or having a potential conflict of interest:

a) Certification including information meetings, planning meetings, examination of documents, auditing (not internal auditing or internal security reviews) and follow up of non-conformities;

b) Arranging and participating as a lecturer in training courses, provided that where these courses relate to information security management, related management systems or auditing. They should confine themselves to the provision of generic information and advice which is freely available in the public domain, i.e. they should not provide company specific advice which contravenes the requirements of c) below;

c) Making available or publishing on request information on the basis for the certification body's interpretation of the requirements of the certification audit standards;

d) Activities prior to audit aimed solely at determining readiness for certification audit; but such activities should not result in the provision of recommendations or advice that would contravene this clause and the certification body should be able to confirm that such activities do not contravene these requirements and that they are not used to justify a reduction in the eventual certification audit duration;

e) Performing second and third party audits according to other standards or regulations than those being part of the scope of accreditation;

f) Adding value during certification audits and surveillance visits, e.g., by identifying opportunities for improvement, as they become evident, during the audit without recommending specific solutions.

The certification body shall be independent from the body or bodies (including any individuals) which provide the internal audit or internal security review of the client organization's ISMS subject to certification.

### 5.3 Liability and financing

**ISO/IEC 17021 Clause 5.3 states requirements for certification bodies to cover liabilities and ensure necessary financial resources.**

# 6. Structural requirements

### 6.1 Organizational structure and top management

**ISO/IEC 17021 Clause 6.1 states requirements for documenting the organizational structure of the certification body.**

***ISMS Specific Guidance***

**G 6.1 Confidence**

Certification of an ISMS shall give adequate confidence that the system meets specified requirements. A certification of conformity of a client organization's ISMS shall demonstrate that a client organization has implemented and is maintaining an effective ISMS in the area specified on the certificate, and is operating its processes in accordance with that system.

The certification body shall ensure that activities of related bodies do not affect the confidentiality, objectivity, or impartiality of its certifications and shall not offer or provide

a) Those services that it certifies/registers others to perform;

b) Consulting services to obtain or maintain certification;

c) Services to design, implement or maintain ISMS or related management systems.

### 6.2 Committee for safeguarding impartiality

**ISO/IEC 17021 Clause 6.2 states the requirement for a committee safeguarding impartiality within the certification body.**

# 7. Resource requirements

## 7.1 Competence of management and personnel

**ISO/IEC 17021 Clause 7.1 states requirements for the competence of management and personnel of the certification body.**

***ISMS Specific Guidance***

**G 7.1 Management competence**

The emphasis in this guidance is placed on the competence of the certification body to direct and manage the certification process. The essential elements of competence required to perform ISMS certification are to select, provide and manage those individuals whose individual and collective competence is appropriate to the activities to be audited and the related information security issues.

Competence analysis

The certification body shall ensure knowledge of the technological and legal developments relevant to the ISMS of the client organization, which it assesses.

The certification body shall have an effective system for the analysis of the competencies in information security management, which it needs to have available, with respect to all the technical areas in which it operates.

Contract review

For each client, the certification body shall be able to demonstrate that it has performed a competence analysis (assessment of skills in response to evaluated needs) of the requirements of each relevant sector prior to undertaking the contract review. The certification body shall then review the contract with the client organization, based on the results of this competence analysis. In particular, the certification body shall be able to demonstrate that it has the competence to complete the following activities:

a) Understand the areas of activity of the client organization and the associated business risks;

b) Define the competencies needed in the certification body to certify in relation to the identified activities, and information security related threats to assets, vulnerabilities and impacts on the client organization;

c) Confirm the availability of the required competencies.

Resources

The management of the certification body shall have the resources to enable it to determine whether or not individual auditors are competent for the tasks they are required to perform within the scope of certification in which they are operating. The certification body shall also have procedures in place to ensure that. The competence of auditors may be established by verified background experience and specific training or briefing (see also Annex A.2). The certification body should be able to communicate effectively with all those whose services it uses.

## 7.2 Personnel involved in the certification activities

**ISO/IEC 17021 Clause 7.2 states requirements for the competence of personnel of the certification body involved in the certification activities.**

***ISMS Specific Guidance***

**G 7.2 Competence of certification body personnel**

Certification bodies shall have personnel competent to:
a) Select and verify the competence of ISMS auditors for audit teams appropriate for the audit;
b) Brief ISMS auditors and arrange any necessary training;
c) Decide on the granting, maintaining, withdrawing, suspending, extending, or reducing of certifications;
d) Set up and operate an appeals, complaints and disputes procedure.

Auditors shall meet the requirements of the appropriate international documentation. For the certification audit of an ISMS, relevant guidelines for auditing are found in ISO 19011.

Training and selection of audit teams

When required, the audit team may be supplemented by technical experts who can demonstrate specific competence in a field of technology appropriate to the audit - note should be taken that technical experts cannot be used in place of ISMS auditors. The certification body shall have a procedure for:
a) Selecting auditors and technical experts on the basis of their competence, training, qualifications and experience;
b) Initially assessing the conduct of auditors and technical experts during certification audits and subsequently monitoring the performance of auditors and technical experts.

When selecting the audit team to be appointed for a specific certification audit the certification body shall ensure that the skills brought to each assignment are appropriate. The team shall:
a) Have appropriate technical knowledge of the specific activities for which certification is sought and, where relevant, with associated procedures and their potential to cause information security failure (technical experts who are not auditors may fulfil this function);
b) Have a degree of understanding sufficient to make a reliable certification audit of the competence of the client organization to manage the information security aspects of its activities, products and services.

In addition, the certification body shall have criteria for the training and selection of audit teams that ensures:
a) Knowledge of the ISMS standard and normative documents;
b) Understanding of information security;
c) Understanding of risk assessment and risk management from the business perspective;
d) Technical knowledge of the activity to be audited;
e) Knowledge of regulatory requirements relevant to the ISMS;
g) Management system knowledge;
h) Knowledge of measurement of control effectiveness.

These training requirements apply to all members of the audit team, with the exception of d), which can be shared among members of the audit team.

Management of the decision taking process

The management function shall have the technical competence and ability in place to manage the process of decision taking regarding the granting, maintaining, extending, reducing, suspending and withdrawing of ISMS certification to the requirements of ISO/IEC 27001.

Pre-requisite levels of education, work experience, auditor training and audit experience for auditors conducting ISMS audits

Persons employed by certification bodies for performing audits of ISMS by themselves shall comply with the following criteria, based on ISO 19011. The following attributes should be considered for each member of the ISMS audit team, except technical experts, and the audit team leader should comply with each of them:

a) Education at secondary level;

b) At least four years full time practical workplace experience in information technology, of which at least two years in a role or function relating to information security;

c) The successful completion of five day training, the scope of which covers ISMS audits and audit management shall be considered appropriate;

d) Prior to assuming responsibility for performing as an auditor, the candidate shall have gained experience in the entire process of assessing information security. This experience shall have been gained by participation in a minimum of four certification audits for a total of at least 20 days, including review of documentation and risk analysis, implementation assessment and audit reporting;

e) All relevant experience shall be reasonably current;

f) The candidate shall be able to put complex operations in a broad perspective and shall be able to understand the role of individual units in larger client organizations;

g) Keep their knowledge and skills in information security and auditing up to date through continual professional development.

Auditors performing as lead auditor shall additionally fulfil the following requirements, which shall be demonstrated in audits under guidance and supervision:

h) Knowledge and attributes to manage the certification audit process;

i) Have acted as auditor in at least three complete ISMS audits;

j) Have demonstrated to possess adequate knowledge and attributes to manage the certification audit process;

k) Have demonstrated the capability to communicate effectively, both orally and in writing.

## 7.3 Use of individual external auditors and external technical experts

**ISO/IEC 17021 Clause 7.3 states requirements for the use of external individuals in the certification process.**

***ISMS Specific Guidance***

**G 7.3 Subcontracting**

When subcontracting, the certification body shall ensure that the subcontracted body or person is competent and complies with the applicable provisions of this publication and is not involved, either directly or through its employer with the design, implementation or maintenance of a ISMS or related management system(s) in such a way that impartiality could be compromised.

Use of Technical Experts

Technical experts with specific knowledge regarding the process and information security issues and legislation affecting the client organization, but who do not satisfy all of the above criteria, may be part of the audit team. Technical experts should not function independently.

## 7.4 Personnel records

**ISO/IEC 17021 Clause 7.4 states requirements for the certification body regarding the management of personnel records.**

## 7.5 Outsourcing

**ISO/IEC 17021 Clause 7.5 states requirements for the certification body if the body wants to use outsourcing.**

# 8. Information requirements

## 8.1 Publicly accessible information

**ISO/IEC 17021 Clause 8.1 states requirements for making information publicly accessible.**

***ISMS Specific Guidance***

**G 8.1 Procedures for granting, maintaining, extending, reducing, suspending and withdrawing certification**

The certification body shall specify the conditions for granting, maintaining, reducing and extending certification and the conditions under which certification may be suspended or withdrawn, partially or in total, for all or part of the client organization's scope of certification. In particular, the certification body shall require the client organization to notify it promptly of any intended changes to the ISMS or other changes, which may affect conformity.

The certification body shall require the client organization to have a documented and implemented ISMS which conforms to applicable ISMS standards or other normative documents.

The certification body shall have documented procedures, which shall be made available on request for:

a) The initial certification audit of a client organization's ISMS, in accordance with the provisions of ISO 19011, ISO/IEC 17021 and other relevant documents;
b) Surveillance and recertification audits of a client organization's ISMS in accordance with ISO 19011 and ISO/IEC 17021 on a periodic basis for continuing conformity with relevant requirements and for verifying and recording that a client organization takes corrective action on a timely basis to correct all nonconformities.

## 8.2 Certification documents

**ISO/IEC 17021 Clause 8.2 states requirements for the documents related to certification.**

***ISMS Specific Guidance***

**G 8.2 ISMS Certification documents**

The certification body shall provide to each of its client organizations whose ISMS is certified, certification documents such as a letter or a certificate signed by an officer who has been assigned such responsibility. For the client organization and each of its information systems covered by the certification, these documents shall identify the scope of the certification granted, including the normative ISMS standard ISO/IEC 27001 to which ISMS are certified, and a reference to the specific version of the Statement of Applicability;

## 8.3 Directory of certified clients

**ISO/IEC 17021 Clause 8.3 states the requirement to maintain a directory of certified clients.**

## 8.4 Reference to certification and use of marks

**ISO/IEC 17021 Clause 8.4 states requirements and constraints for the reference to certification and the use of marks.**

***ISMS Specific Guidance***

**G 8.4 Control of certification marks**

The certification body shall exercise proper control over ownership, use and display of its ISMS certification marks. If the certification body confers the right to use a symbol or logo to indicate certification of an ISMS, the certification body should ensure that the client organization may use the specified symbol or logo only as authorised in writing by the certification body. This symbol or logo shall not be used on a product, or in a way that may be interpreted as denoting product conformity.

## 8.5 Confidentiality

**ISO/IEC 17021 Clause 8.5 states requirements for the certification body to maintain confidentiality, where required.**

***ISMS Specific Guidance***

**G 8.5 Access to organizational records**

Before the certification audit, the client organization should be asked to advise if any ISMS records cannot be made available for review by the audit team because they contain confidential or sensitive information. The certification body shall determine whether the ISMS can be adequately assessed in the absence of these records. If the certification body concludes that it is not possible to adequately assess the ISMS without reviewing the identified confidential or sensitive records, the client organization should be advised that the certification audit cannot take place until appropriate access arrangements are agreed.

## 8.6 Information exchange between a certification body and its clients

**ISO/IEC 17021 Clause 8.6 states requirements on the information exchange between the certification body and its clients. This clause includes**

**8.6.1 Information on the certification activity and requirements**

**8.6.2 Notice of changes by a certification body**

**8.6.3 Notice of changes by a client**

# 9. Process requirements

## 9.1 General requirements applicable to any audit

**ISO/IEC 17021 Clause 9.1 states general audit requirements.**

***ISMS Specific Guidance***

**G 9.1 (1) General ISMS audit requirements**

Certification audit criteria

The criteria against which the ISMS of an applicant are assessed shall be those outlined in the ISMS standard or other normative documents relevant to the function performed. If an explanation is required as to the application of these documents to a specific certification programme, it shall be formulated by relevant and impartial committees or persons possessing the necessary technical competence and published by the certification body.

Policies and procedures

The documentation of the certification body shall include the policy and procedures for implementing the certification process, including checks of the use and application of documents used in certification of ISMS and the procedures for assessing and certifying the client organization's ISMS.

Audit team

The audit team shall be formally appointed and provided with the appropriate working documents. The plan for and the date of the audit shall be agreed to with the client organization. The mandate given to the audit team shall be clearly defined and made known to the client organization, and shall require the audit team to examine the structure, policies and procedures of the client organization, and confirm that these meet all the

requirements relevant to the scope of certification and that the procedures are implemented and are such as to give confidence in the ISMS of the client organization.

**G 9.1 (2) Scope of certification**

The audit team shall assess the ISMS of the client organization covered by the defined scope against all applicable certification requirements. The certification body shall ensure that the scope and boundaries of the ISMS of the client organization are clearly defined in terms of the characteristics of the business, the organization, its location, assets and technology. The role of the certification body is to confirm that the client organizations address the requirements stated in Section 1.2 of ISO/IEC 27001 in the scope of their ISMS.

Certification bodies shall therefore ensure that the client organization's information security risk assessment properly reflects its activities and extends to the boundaries of its activities as defined in the normative ISMS standard ISO/IEC 27001. Certification bodies shall confirm that this is reflected in the client organization's scope of their ISMS and Statement of Applicability.

Certification bodies shall ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to certification and are included in the client organization's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. computers, telecommunication systems, etc.) with others.

**G 9.1 (3) Multiple sites**

Multiple site sampling decisions in the area of ISMS certification are more complex than the same decisions are for quality systems. Certification bodies wishing to use a sample based approach to multiple site certification audit need to maintain procedures, which include the full range of issues below in the building of their sampling programme.

The certification body's procedures should ensure that the initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined in accordance with the provisions below. Where a client organization has a number of similar sites covered by a single ISMS, a certificate may be issued to the client organization to cover all such sites provided that:

a) All sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review;

b) All sites are included within the client organization's internal ISMS audit scope and that the basis for sampling can be justified;

c) All sites are included within the client organisation's ISMS management review programme;

d) A representative number of sites have been sampled by the certification body, taking into account:

- i) The results of internal audits of head office and the sites,
- ii) The results of management review,
- iii) Variations in the size of the sites,

iv) Variations in the business purpose of the sites,
v) Complexity of the ISMS,
vi) Complexity of the information systems at the different sites,
vii) Variations in working practices,
viii) Variations in activities undertaken,
ix) Potential interaction with critical information systems or information systems processing sensitive information,
x) Any differing legal requirements;

d) The sample should be partly selective based on the above in point c) and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection;
e) every site included in the ISMS which is subject to significant risks should be audited by the certification body prior to certification;
f) The surveillance programme should be designed in the light of the above requirements and should, within a reasonable time, cover all sites of the client organization or within the scope of the ISMS certification;
g) in the case of a nonconformity being observed either at the head office or at a single site, the corrective action procedure should apply to the head office and all sites covered by the certificate.

The audit described in G 9.1 (4) below shall address the client organization's head office activities to ensure that a single ISMS applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above.

**G 9.1 (4) Audit Methodology**

A certification body shall perform its audit of a client organization’s ISMS in at least two stages at the client organization’s site(s), unless it can justify an alternative approach. Adaptation of the certification process to the needs of very small client organizations may provide justification in particular circumstances. For the purposes of this guidance, two stages are described as "audit (stage 1)" and "audit (stage 2)". The key objectives of each, together with the minimum coverage, are described in G 9.2.3 (1) and G 9.2.3 (2).

The certification body should have procedures, which require that the client organization to be able to demonstrate that the internal ISMS audit is scheduled, and the programme and procedures are operational and can be shown to be operational.

The certification body’s procedures should not presuppose a particular manner of implementation of an ISMS or a particular format for documentation and records. Certification procedures should focus on establishing that a client organization’s ISMS meets the requirements of the ISO/IEC 27001 standard and the policies and objectives of a client organization.

**G 9.1 (5) Certification Audit Report**

The certification body may adopt reporting procedures that suit its needs but as a minimum these procedures shall ensure that:

a) A meeting takes place between the audit team and the client organization's management prior to leaving the premises at which the audit team provides:

(i) A written or oral indication regarding the conformity of the client organization's ISMS with the particular certification requirements;

(ii) An opportunity for the client organization to ask questions about the findings and their basis;

b) The audit team provides the certification body with a report of its findings as to the conformity of the client organization's ISMS with all of the certification requirements;

c) The report shall contain, as a minimum, comments on the conformity of the client organization's ISMS with the certification requirements with a clear statement of nonconformity and, where applicable, any useful comparison with the results of previous certification audits of the client organization,

The report shall consider the adequacy of the internal organization and procedures adopted by the client organization to give confidence in the ISMS.

In addition to the requirements for reporting in ISO/IEC 17021, this information should cover:

- the degree of reliance that can be placed on the internal security reviews;
- a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS;
- the conclusions reached by the audit team.

## 9.2 Initial audit and certification

**ISO/IEC 17021 Clause 9.2 states the requirements for the process of the initial audit and the certification that could follow from that. This clause contains several sub-clauses which are cited below.**

**9.2.1 Application and 9.2.2 Application review**

***ISMS Specific Guidance***

**G 9.2 (1) Audit Team competence**

The following requirements apply to certification assessment. For surveillance activities only those requirements which are relevant to the scheduled surveillance activity apply.

The following requirements apply to each member of the audit team, except technical experts:

all members of the audit team shall be able to demonstrate competence in all of the following:

a) The normative ISMS standard ISO/IEC 27001;

b) The concepts of management systems in general;

c) Issues related to various areas of information security;

d) The principles and processes related to risk assessment and risk management;

e) Principles of auditing based on ISO 19011.

The following requirements apply to the audit team as a whole:

a) In each of the following areas at least one audit team member should satisfy the certification body's criteria for taking responsibility within the team:

- i) Managing the team,
- ii) Management systems and process applicable to ISMS,
- ii) Knowledge of the legislative and regulatory requirements in the particular information security field,
- iii) Identifying information security related threats and incident trends,
- iv) Identifying the vulnerabilities of the client organization and understanding the likelihood of their exploitation, their impact and their mitigation and control,
- v) ISMS controls and their implementation,
- vi) Related and/or relevant ISMS standards, industry best practices, security policies and procedures,
- vii) Incident handling methods and business continuity,
- viii) Knowledge about tangible and intangible information assets and impact analysis,
- ix) Knowledge of the current technology where security might be relevant or an issue,
- vi) Knowledge of risk management processes and methods;

b) The audit team should be competent to trace indications of security incidents in the client organization's ISMS back to the appropriate elements of the ISMS;

c) An audit team may consist of one person provided that the person meets all the criteria set out in a) above;

d) Appropriate work experience and practical application of the items above (this does not mean that an auditor needs a complete range of experience of all areas of information security, but the audit team as whole should have enough appreciation and experience to cover the ISMS scope being audited):

- (i) Work experience (new, real practical experience);
- (ii) Having a working experience, awareness and understanding on how to apply the knowledge.

<u>Demonstration of Auditor Competence</u>

Auditors shall be able to demonstrate their knowledge and experience, as outlined above, for example through:

a) Recognised ISMS-specific qualifications;

b) Registration as auditor;

c) Approved ISMS training courses;

d) Up to date continuous professional development records;

e) Practical demonstration through witnessing auditors going though the ISMS audit process on real client systems.

**G 9.2 (2) General Preparations for the Initial Audit**

The certification body shall require that a client organization makes all necessary arrangements for the conduct of the certification audit, including provision for examining documentation and the access to all areas, records (including internal audit reports and reports of independent reviews of information security) and personnel for the purposes of certification audit, recertification audit and resolution of complaints.

At least the following information shall be provided by the applicant prior to the onsite certification audit:
a) General information concerning the ISMS and the activities it covers;
b) A copy of the ISMS manual and, where required, the associated documentation.

**9.2.3 Initial certification audit**

***ISMS Specific Guidance***

**G 9.2.3 (1) Audit (stage 1)**

In this stage of the audit, the certification body shall obtain documentation on the design of the ISMS covering the documentation required in Clause 4.3.1 of ISO/IEC 27001.

The objectives of the audit (stage 1) are to provide a focus for planning the audit (stage 2) by gaining an understanding of the ISMS in the context of the client organization's ISMS policy and objectives, and, in particular, of the client organization's state of preparedness for the audit.

The audit (stage 1) includes, but should not be restricted to, the document review. The certification body shall agree with the client organization when and where the document review is conducted. In every case, the document review should be completed prior to the commencement of audit (stage 2).

The results of the audit (stage 1) should be documented in a written report. The certification body should review the audit (stage 1) report for deciding on proceeding with the audit (stage 2) and for selecting audit (stage 2) team members with the necessary competence.

The certification body should make the client organization aware of the further types of information and records that may be required for detailed inspection during the audit (stage 2).

**G 9.2.3 (2) Audit (stage 2)**

The audit (stage 2) always takes place at the site(s) of the client organization. On the basis of findings documented in the audit (stage 1) report, the certification body drafts an audit plan for the conduct of the audit (stage 2). The objectives of the audit (stage 2) are:
a) To confirm that the client organization adheres to its own policies, objectives and procedures;
b) To confirm that the ISMS conforms with all the requirements of the normative ISMS standard ISO/IEC 27001 and is achieving the client organization’s policy objectives;
To do this, the audit should focus on the client organization's

a) Assessment of information security related risks, and that the assessments produce comparable and reproducible results;
b) The document requirements listed in Section 4.3.1 of ISO/IEC 27001.
c) Selection of control objectives and controls based on the risk assessment and risk treatment processes;
d) Reviews of the effectiveness of the ISMS and measurements of the effectiveness of the information security controls, reporting and reviewing against the ISMS objectives;
e) Internal ISMS audits and management reviews;
f) Management responsibility for the information security policy;
g) Correspondence between the selected and implemented controls, the Statement of Applicability, and the results of the risk assessment and risk treatment process, and the ISMS policy and objectives;
h) Implementation of controls (see Annex A.4), taking into account the organization's measurements of effectiveness of controls (see f)), to determine whether controls are implemented and effective to achieve the stated objectives;
i) Programmes, processes, procedures, records, internal audits, and reviews of the ISMS effectiveness to ensure that these are traceable to management decisions and the ISMS policy and objectives.

**G 9.2.3 (3) Specific Elements of the ISMS Audit**

The role of the certification body is to establish that client organizations are consistent in establishing and maintaining procedures for the identification, examination and evaluation of information security related threats to assets, vulnerabilities and impacts on the client organization. Certification bodies shall consider the following factors:
a) The certification body shall require the client organization to demonstrate that the analysis of security related threats is relevant and adequate for the operation of the client organization;
Note: The client organization is responsible for defining criteria by which information security related threats to assets, vulnerabilities and impacts on the client organization are identified as significant, and to develop procedure(s) for doing this;
b) The certification body shall establish whether the client organization’s procedures for the identification, examination and evaluation of information security related threats to assets, vulnerabilities and impacts and the results of their application are consistent with the client organization’s policy, objectives and targets.

The certification body should establish whether the procedures employed in analysis of significance are sound and properly implemented. If an information security related threat to assets, a vulnerability, or an impact on the client organization is identified as being significant, it shall be managed within the ISMS.

<u>Regulatory Compliance</u>

The maintenance and evaluation of legal compliance is the responsibility of the client organization. The certification body should restrict itself to checks and samples in order to establish confidence that the ISMS functions in this regard. The certification body should verify that the client organization has a management system to achieve legal and regulatory compliance applicable to the information security risks and impacts.

Integration of ISMS documentation with that for Other Management Systems

The client organization can combine the documentation for ISMS and other management systems (such as quality, health and safety, and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems.

Combining Management System Audits

A certification body may offer other management system certification linked with ISMS certification, or may offer ISMS certification only.

The ISMS audit can be combined with audits of other management systems. This combination is possible provided it can be demonstrated that the audit satisfies all requirements for certification of the ISMS. All the elements important to an ISMS should appear clearly, and be readily identifiable, in the audit reports. The quality of the audit should not be adversely affected by the combination of the audits.

Note: ISO 19011 provides guidance for carrying out combined management system audits.

Certification decision

The decision whether or not to certify a client organization's ISMS shall be taken by the certification body on the basis of the information gathered during the certification process and any other relevant information. Those who make the certification decision shall not have participated in the audit.

The entity which takes the decision on granting certification should not normally overturn a negative recommendation of the audit team. If such a situation does arise, the certification body shall document and justify the basis for the decision to overturn the recommendation.

On the subject of deciding on certification, ISO/IEC 17021 does not mention a specific period in which at least one complete internal audit and one management review and one security review of the client organization’s ISMS shall have taken place. The certification body may specify a period. Irrespective of whether the certification body has chosen to specify a minimum frequency, measures shall be established by the certification body to ensure the effectiveness of the client organization’s management review, security review and internal audit processes.

Certification shall not be granted to the client organization until there is sufficient evidence to demonstrate that the arrangements for management and security reviews have been implemented, are effective and will being maintained.

**9.2.4 Initial certification audit reports, 9.2.5 Post-audit activities and 9.2.6 Initial certification decision granting or extending certification**

***ISMS Specific Guidance***

**G 9.2.4 (1) Reporting by audit teams to the certification body**

In order to provide a basis for the certification decision, the certification body shall require clear reports, which provide sufficient information to make the decision.

a) Reports from the audit team to the certification body are required at various stages in the certification audit process. In combination with information held on file, these reports should at least contain:

i) an account of the audit including a summary of the document review,

ii) an account of the certification audit of the client organization's information security risk analysis,

iii) total audit time used and detailed specification of time spent on document review, assessment of risk analysis, implementation audit, and audit reporting,

iv) clarification of nonconformities,

v) audit enquiries which have been followed, rationale for their selection, and the methodology employed,

vi) recommendation on certification by the audit team to the certification body;

b) A surveillance report should contain, in particular, information on clearing of nonconformities revealed previously. As a minimum, the reports arising from surveillance should build up to cover in totality the requirement of point a) above.

**G 9.2.4 (2) Decision taking, in relation to the certification function**

The entity, which may be an individual, which takes the decision on granting/withdrawing a certification within the certification body, should incorporate a level of knowledge and experience in all areas which is sufficient to evaluate the audit processes and associated recommendations made by the audit team.

## 9.3 Surveillance activities

**ISO/IEC 17021 Clause 9.3 states the requirements for surveillance activities. This clause includes:**

**9.3.1 General**

**9.3.2 Surveillance audit**

**9.3.3 Surveillance audit report**

**9.3.4 Maintaining certification**

***ISMS Specific Guidance***

**G 9.3 Surveillance audits and recertification audits**

The certification body shall carry out periodic surveillance and recertification audit at sufficiently close intervals to verify that its client organizations whose ISMS are certified continue to comply with the certification requirements.

Note: In most cases it is unlikely that a period greater than one year for periodic surveillance would satisfy the requirements of this clause.

Surveillance and recertification audit procedures shall be consistent with those concerning the certification audit of the client organization's ISMS as described in this standard.

The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of changes to that system initiated as a result of changes in the client organization's operation and to confirm continued compliance with certification requirements. Surveillance of a client organization's ISMS shall take place on a regular basis; normally it should be undertaken at least once a year. Surveillance programs should normally include:
a) The system maintenance elements which are internal audit, internal security review, management review and preventive and corrective action;
b) Communications from external parties as required by the ISMS standard or normative document;
c) Changes to the documented system;
d) Areas subject to change;
e) Selected elements of ISO/IEC 27001;
f) Other selected areas as appropriate.

As a minimum, surveillance by the certification body shall, on an annual basis, review the following:
a) The effectiveness of the ISMS with regard to achieving the objectives of the client organization's information security policy;
b) The functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;
c) Action taken on nonconformities identified during the last audit.
Surveillance by the certification body should at least cover the points listed for reporting in ISO/IEC 17021.

In addition, the following issues should be considered:
a) The certification body should be able to adapt its surveillance programme to the information security issues related threats to assets, vulnerabilities and impacts on to the client organization and justify this programme.
b) The surveillance programme of the certification body should be determined by the certification body. Specific dates for visits may be agreed with the certified client organization.
c) Surveillance audits may be combined with audits of other management systems. The reporting should clearly indicate the aspects relevant for each management system.
d) The certification body is required to supervise the appropriate use of the certificate and report.
e) The audit methodology for recertification audits should be the same as for audit (stage 2).

During surveillance audits, certification bodies should check the records of appeals, complaints and disputes brought before the certification body, and where any nonconformity or failure to meet the requirements of certification is revealed, that the client organization has investigated its own ISMS and procedures and taken appropriate corrective action.

## 9.4 Recertification

**ISO/IEC 17021 Clause 9.4 states the requirements for the recertification process. This clause includes:**

**9.4.1 Recertification cycle**

**9.4.2 Recertification audit plan**

**9.4.3 Recertification audit**

**9.4.4 Recertification audit report**

**9.4.5 Recertification decision**

***ISMS Specific Guidance***

**G 9.4 Recertification audits**

If, exceptionally, the recertification audit period is extended beyond three years, the certification body should demonstrate that the effectiveness of the complete ISMS has been evaluated on a regular basis, and should have a surveillance frequency that compensates for this in order to maintain the same level of confidence.

Certification bodies shall have clear procedures laying down the circumstances and conditions in which certifications will be maintained. If on surveillance or recertification audit, nonconformities are found to exist, such nonconformities shall be effectively corrected within a time agreed by the certification body. If correction is not made within the time agreed certification shall be reduced, suspended or withdrawn. The time allowed to implement corrective action should be consistent with the severity of the nonconformity and the risk to the assurance of products or services meeting specified requirements.

## 9.5 Special audits

**ISO/IEC 17021 Clause 9.5 states the requirements for special audits, e.g. in cases of complaints.**

***ISMS Specific Guidance***

**G 9.5 Special cases**

The surveillance activities shall be subject to special provision if a client organization with a certified ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification.

If, exceptionally, the recertification audit period is extended beyond three years, the certification body should demonstrate that the effectiveness of the complete ISMS has been evaluated on a regular basis, and should have a surveillance frequency that compensates for this in order to maintain the same level of confidence.

## 9.6 Suspending, withdrawing or reducing scope of certification

**ISO/IEC 17021 Clause 9.6 states requirements for the case where the scope of certification is changed.**

## 9.7 Appeals

**ISO/IEC 17021 Clause 9.7 states the requirements for the appeals process.**

## 9.8 Complaints

**ISO/IEC 17021 Clause 9.8 states the requirements for the complaints process.**

***ISMS Specific Guidance***

**IG 9.8 Surveillance audits and recertification audits**

Complaints represent a source of information as to possible nonconformity. On receipt of a complaint the certified client organization should establish, and where appropriate report on, the cause of the nonconformity, including any predetermining (or predisposing) factors within the client organization's ISMS.

The certification body should satisfy itself that the client organization is using such investigations to develop remedial / corrective action, which should include measures for:

- notification to appropriate authorities if required by regulation;
- restoring conformity as quickly as possible;
- preventing recurrence;
- evaluating and mitigating any adverse security incidents and their associated impacts;
- ensuring satisfactory interaction with other components of the ISMS;
- assessing the effectiveness of the remedial / corrective measures adopted.

The certification body shall require each client organization whose ISMS is certified to make available to the certification body, when requested, the records of all complaints and corrective action taken in accordance with the requirements of ISO/IEC 27001.

## 9.9 Records on applicants and clients

**ISO/IEC 17021 Clause 9.9 states requirements for the records the certification body needs to maintain.**

# 10. Management system requirements for certification bodies

## 10.1 Option 1 – Management system requirements in accordance with ISO 9001

## 10.2 Option 2 – General management system requirements

**ISO/IEC 17021 Clause 10.2 states typical management system requirements This clause contains:**

**10.2.1 Management system manual**

**10.2.2 Control of documents**

**10.2.3 Control of records**

**10.2.4 Management review**

**10.2.5 Internal audits**

**10.2.6 Corrective action**

**10.2.5 Preventive action**

# Annex A.1 *Analysis of a Client Organization's Complexity and Sector-Specific Aspects*

*(Informative)*

## A.1.1 Organization's Risk Potential

The client organization's complexity needs to be considered when deciding audit time and auditor competence. This annex intends to provide an example in analyzing the complexity of a client organization for this purpose.

The organization complexity category assigned to an organization can then be used to decide:

a) the auditors' competency requirements for the ISMS audit of the organization (an example of which is given in Annex A.2);
b) the audit time requirements for the ISMS audit of the organization (an example of which is given in Annex A.3).

Table A.1 is only a general indication of the possible factors deciding an organization's complexity. It might need to be adapted to specific circumstances or have any special factors included as seen appropriate.

By using the Organization Complexity Criteria (in Table A.1 below), a client organization's complexity can be classified into three categories: "high", "medium", and "low", using a number of different factors. The overall effective category of the organization can be taken as the maximum category of all the factors considered, and the outcome is the category, i.e. "high", "medium" or "low".

**Table A.1 Criteria for Organization Complexity**

| Complexity Factor | Category | | | Significance |
|---|---|---|---|---|
| | High | Medium | Low | |
| Number of employees + contractor staff | ≥1,000 | ≥200 | <200 | • Scale of ISMS implementation<br>• Management information system and OA<br>• Production management-related systems<br>• Sales/distribution/general service-related systems<br>• Information technology/information services and related systems<br>• Construction/ship-building/plant engineering-related systems |
| Number of users | ≥1million | ≥200,000 | < 200,000 | • Financial systems<br>• Governments, Schools, Medicals/hospitals systems |
| Number of sites | ≥5 | ≥2 | 1 | • Scale of ISMS implementation<br>• Physical and environmental security (A.9) |

| | | | | |
|---|---|---|---|---|
| Number of servers | ≥100 | ≥10 | <10 | • Scale of ISMS implementation<br>• Physical and environmental security (A.9),<br>• Access control (A.11),<br>• Telecommunications and operation management (A.10) |
| Number of workstations + PC + laptops | ≥300 | ≥50 | <50 | • Access control (A.11) |
| Number of application development and maintenance staff | ≥100 | ≥ 20 | < 20 | • Information systems acquisition, development and maintenance (A.12) |
| Network & encryption technology | External / internet connection with encryption / digital signature / PKI requirements | External / internet connection without encryption / digital signature / PKI requirements | No external / internet connection | • Telecommunications and operation management (A.10)<br>• Access control (A.11) |
| Significance in legal compliance | Incompliance leads to possible prosecution | Incompliance leads to significant financial penalty or goodwill damage | Incompliance leads to insignificant financial penalty or goodwill damage | • Laws and guidelines (A.15) |
| Applicability of sector specific risk *(refer to Annex A.1.2 for the example of sector specific risk and sector specific law and regulation)* | Sector specific law and regulation applies | No applicable sector specific law and regulation but significant sector specific risk applies | No applicable sector specific law and regulation and no applicable sector specific risk applies | • Scale of ISMS implementation<br>• Laws and guidelines (A.15) |

## A.1.2 Sector Specific Categories of Information Security Risk

**Sector specific risks**, which can be sensitive, critical and /or personal, for example:

- personal sensitive (healthcare, salaries, pensions, education….)
- commercially sensitive/critical (telecoms, finance, automotive, aerospace)
    - examples: research & development information, design information, customers details, financial results and forecasts, business plans, IPR, manufacturing processes….
- government sensitive/critical
    - public information
    - internal and interdepartmental information
    - e-government applications
    - healthcare, social services (benefits and claims), taxes
    - information handled by suppliers and manufacturers of government ICT designs, facilities and products
- Other sensitive/critical sectors
    - Charities and non-profit organizations

**Sector specific laws and regulations**

- Telecoms
- Finance
- Corporate Governance
- Health and Safety

# Annex A.2 *Example Areas of Auditor Competence (Informative)*

## A.2.1 General competence considerations

There are several ways of how an auditor can prove their knowledge and experience. This can, for example, be achieved by using recognised qualifications, such as university degrees, CISA, CISM or CISSP. Registration, e.g. under IRCA or any other recognised form of auditor registration, can also be used to demonstrate the required knowledge and experience.

## A.2.2 Specific competence considerations

### A.2.2.1 Establishing the competence level for conducting audit of the organization's ISMS

The required competence level for the audit team should be established, corresponding with the organization's industry/technological field and complexity factor. Regarding "industry/technological field", the audit team should be required to have specialized technological skills of proficiency A (Adequate) in the same industry/technological field.

However, if the complexity factor is high, the audit team is required to have specialized technological skill level "proficiency E (Expert)." The following relation between complexity factor and competence level should be applied:

| Risk Potential | Competence level (Proficiency class) |
|---|---|
| High | E (Expert) |
| Either medium or low | A (Adequate) |

**A.2.2.2 Knowledge of ISO/IEC 27002 (the renumbered ISO/IEC 17799 as from April 2007) controls**

The following describes the typical knowledge in relation to ISMS auditing. In addition to the control areas from ISO/IEC 27002 (the renumbered ISO/IEC 17799 as from April 2007), which are listed in the following table, auditors should also be aware of the other standards in the 27000 series of standards.

| | |
|---|---|
| Knowledge and experience of policies, business requirements for information security | Security policy |
| General knowledge and experience of business processes, practices and organisational structures. | Organising information security |
| Knowledge of asset valuation, inventories, classifications, acceptable use polices | Asset management |
| General knowledge and experience of the processes and procedures used by human resource departments | Human resources security |
| Knowledge of physical & environmental security | Physical & environmental security |
| Up to date knowledge and experience of the standards, processes, techniques and methods used for information security both management measures as well as some appropriate level of technical expertise. This includes current knowledge of some of the common business practices. | Communications & operations management |
| | Access control |
| | Information systems acquisition, development and maintenance |
| Up to date knowledge and experience of the processes and procedures for incident management | Information security incident management |
| Up to date knowledge and experience of the standards, processes, plans and testing for business continuity | Business continuity management |
| Up to date knowledge of business contractual issues, common laws and regulations related to ISMS | Compliance |

The follows describes typical knowledge in relation to ISMS and auditing:

- Audit programming and planning
- Audit type and methodologies
- Audit risk
- IS Processes analysis
- Deming circle for continuos improvement
- Internal auditing for IS

The follows describes typical knowledge in relation to regulatory requirements:

- Intellectual property
- Protection and retention of organizational records
- Data protection and privacy

- Regulation of cryptographic controls
- Homeland security/anti-terrorism
- Electronic commerce
- Electronic and digital signatures
- Workplace surveillance
- Telecommunications interception and monitoring of data (e.g. e-mail)
- Computer abuse
- Electronic evidence collection
- Penetration testing
- National sector specific requirements (e.g. banking)

The follows describes typical knowledge in relation to management requirements:

- Re-engineering of IS risks
- ICT outsourcing security risks
- Supply chain information security risks

# Annex A.3 *Audit Time*

*(Informative)*

An estimation of auditor time that might be required in a certification audit is helpful to plan the audit, and this annex provides examples of how this estimation can be made. It is important to note that the factors that may affect the necessary time are many and varying. It is therefore not possible to give a definitive direction on how the necessary time can be estimated, and only examples are provided in this annex. The estimation may need to be adjusted if more detailed information is made available, or if factors change.

## A.3.1 Example Criteria

Example of criteria organizations might wish to consider:

- How many users? How many are privileged users/
- Volume and types of information handled and processed (covering sensitive, critical and personal information)
- Number of information systems
- Number of networks (size, fixed, mobile, wireless, external, internal)
- Number of IT platforms
- Number of critical systems
- Remote working
- Number and types of electronic transactions
- Number and size of any development projects
- How many 3rd party services are deployed
- Applicable legislation
- Any sector specific requirements e.g. from Annex A.1.2

## A.3.2 Example Calculation

Auditor Time for Initial Audit

The ideas and calculation bases introduced in this annex are based on reported experience of several certification bodies.

The auditor time for an initial audit can be calculated as the sum of the following factors:

- Auditor days required for the ISMS audit (as described in Table A.3 below), referred to as A;
- 2 additional days to audit the controls from ISO/IEC 27002 (the renumbered ISO/IEC 17799 as from April 2007);
- 1 - 3 days for the document review - this number varies dependent on A;
- 1 - 3 days for the report writing - this number varies dependent on A;
- Additional time for on-site audits, estimated as 0.5 x (number of sites that are visited)
- Consideration of the client organization's complexity, as explained in Annex A.1, where each complexity factor can contribute half a day (if high) or a quarter of a day (if medium or low).

**Table A.3 Guide for process to determine auditor time for initial audit (Audit time chart)**

| Number of employees | Auditor time for initial audit (auditor days) |
|---|---|
| 1-10 | 2 |
| 11-25 | 3 |
| 26-45 | 4 |
| 46-65 | 5 |
| 66-85 | 6 |
| 86-125 | 7 |
| 126-175 | 8 |
| 176-275 | 9 |
| 276-425 | 10 |
| 426-625 | 11 |
| 626-875 | 12 |
| 876-1175 | 13 |
| 1176-1550 | 14 |
| 1551-2025 | 15 |
| 2026-2675 | 16 |
| 2676-3450 | 17 |
| 3451-4350 | 18 |
| 4351-5450 | 19 |
| 5451-6800 | 20 |

| | |
|---|---|
| 6801-8500 | 21 |
| 8501-10700 | 22 |
| >10700 | follow progression above |

# Annex A.4 *Harmonised Implementation of Controls*

# *(Informative)*

## A.4.1 Purpose of Annex A.4

This annex provides guidance for the review of the implementation of controls listed in ISO/IEC 27001, Annex A, during an ISMS Certification Audit. The implementation of all controls selected by the client organization (as per the Statement of Applicability) needs to be reviewed in the certification audit (stage 2 audit). Table A.4 below classifies controls into "organizational" vs. "technical" and distinguishes whether a visual inspection or system testing is required to assess the control effectiveness.

## A.4.2 How to use Table A.4

**Columns "organizational control" and "technical control"**

An "X" in the respective column indicates whether the control is primarily an organizational or a technical control. Some controls are both organizational and technical.

Organizational controls can be audited through review of process documentation, interviews, observation and physical inspection. The effectiveness of technical controls can often be audited through system testing (see below) or through use of specialized audit/reporting tools.

**Column "system testing"**

"System testing" means direct review of systems (e.g. review of system settings or configuration). Questions of the auditor could be answered at the system console or by evaluation of the results of testing tools. If the customer has a computer-based tool in use that is known to the auditor, this can be used to support the audit, or the results of an evaluation performed by the customer can be reviewed.

We distinguish three categories for the review of technical controls:

- "possible": system testing is possible for the evaluation of control effectiveness, but usually not necessary;
- "recommended": system testing is usually necessary and should be carried out, but may be omitted if justified (the reasons for omissions should however be documented by the auditor); and
- "required": system testing is mandatory.

**Column "visual inspection"**

An "X" in the column "Visual Inspection" indicates that this control usually requires a visual inspection to evaluate it's effectiveness. This means that it is not sufficient to review the respective process on paper or through interviews – the auditor needs to "see with his own eyes".

**Table A.4 Classification of controls**

| Controls in ISO/IEC 27001:2005, Appendix 1 | | Organizational control | Technical control | System testing<br>*possible*<br>*recommended*<br>*required* | Visual inspection | Comment |
|---|---|---|---|---|---|---|
| A.5 | Security Policy | | | | | |
| A.5.1 | Information Security Policy | | | | | |
| A.5.1.1 | Information security policy document | X | | | | |
| A.5.1.2 | Review of the information security policy | X | | | | |
| A.6 | Organization of information security | | | | | |
| A.6.1 | Internal organization | | | | | |
| A.6.1.1 | Management commitment to information security | X | | | | |
| A.6.1.2 | Information security co-ordination | X | | | | |
| A.6.1.3 | Allocation of information security responsibilities | X | | | | |
| A.6.1.4 | Authorization process for information processing facilities | X | | | | check inventory |
| A.6.1.5 | Confidentiality agreements | X | | | | |
| A.6.1.6 | Contact with authorities | X | | | | |
| A.6.1.7 | Contact with special interest groups | X | | | | |
| A.6.1.8 | Independent review of information security | X | | | | |
| A.6.2 | External parties | | | | | |
| A.6.2.1 | Identification of risks related to external parties | X | | | | |
| A.6.2.2 | Addressing security when dealing with customers | X | | | | |
| A.6.2.3 | Addressing security in third party agreements | X | | | | |
| A.7 | Asset management | | | | | |
| A.7.1 | Responsibility for assets | | | | | |
| A.7.1.1 | Inventory of assets | X | | | | establish inventory |
| A.7.1.2 | Ownership of assets | X | | | | |
| A.7.1.3 | Acceptable use of assets | X | | | | |
| A.7.2 | Information classification | | | | | |

| Controls in ISO/IEC 27001:2005, Appendix 1 | | Organizational control | Technical control | System testing<br>*possible*<br>*recommended*<br>*required* | Visual inspection | Comment |
|---|---|---|---|---|---|---|
| A.7.2.1 | Classification guidelines | **X** | | | | |
| A.7.2.2 | Information labeling and handling | **X** | | | | naming: directories, files, printed reports, recorded media (e.g. tapes, disks, CDs), electronic messages and file transfers. |
| A.8 | Human resources security | | | | | |
| A.8.1 | Prior to employment | | | | | |
| A.8.1.1 | Roles and responsibilities | **X** | | | | |
| A.8.1.2 | Screening | **X** | | | | |
| A.8.1.3 | Terms and conditions of employment | **X** | | | | |
| A.8.2 | During employment | | | | | |
| A.8.2.1 | Management responsibilities | **X** | | | | |
| A.8.2.2 | Information security awareness, education and training | **X** | | | | |
| A.8.2.3 | Disciplinary process | **X** | | | | |
| A.8.3 | Termination or change of employment | | | | | |
| A.8.3.1 | Termination responsibilities | **X** | | | | |
| A.8.3.2 | Return of assets | **X** | | | | |
| A.8.3.3 | Removal of access rights | **X** | **X** | recommended | | |
| A.9 | Physical and environmental security | | | | | |
| A.9.1 | Secure areas | | | | | |
| A.9.1.1 | Physical security perimeter | **X** | | | | |
| A.9.1.2 | Physical entry controls | **X** | **X** | possible | **X** | archiving of access lists |
| A.9.1.3 | Securing offices, rooms and facilities | **X** | | | **X** | |
| A.9.1.4 | Protecting against external and environmental threats | **X** | | | **X** | |
| A.9.1.5 | Working in secure areas | **X** | | | **X** | |
| A.9.1.6 | Public access, delivery and loading areas | **X** | | | **X** | |

| Controls in ISO/IEC 27001:2005, Appendix 1 | | Organizational control | Technical control | System testing<br>*possible*<br>*recommended*<br>*required* | Visual inspection | Comment |
|---|---|---|---|---|---|---|
| A.9.2 | Equipment security | | | | | |
| A.9.2.1 | Equipment siting and protection | X | X | | X | fire detectors in data centers and main cable ducts |
| A.9.2.2 | Supporting utilities | X | X | | X | |
| A.9.2.3 | Cabling security | X | | | X | |
| A.9.2.4 | Equipment maintenance | X | | | | |
| A.9.2.5 | Security of equipment offpremises | X | | | | |
| A.9.2.6 | Secure disposal or re-use of equipment | X | | | X | |
| A.9.2.7 | Removal of property | X | | | | |
| A.10 | Communications and operations management | | | | | |
| A.10.1 | Operational procedures and responsibilities | | | | | |
| A.10.1.1 | Documented operating procedures | X | | | | |
| A.10.1.2 | Change management | X | X | recommended | | |
| A.10.1.3 | Segregation of duties | X | | | | |
| A.10.1.4 | Separation of development, test and operational facilities | X | X | possible | | |
| A.10.2 | Third party service delivery management | | | | | |
| A.10.2.1 | Service delivery | X | | | | |
| A.10.2.2 | Monitoring and review of third party services | X | | | | |
| A.10.2.3 | Managing changes to third party services | X | | | | |
| A.10.3 | System planning and acceptance | | | | | |
| A.10.3.1 | Capacity management | X | | | | |
| A.10.3.2 | System acceptance | X | | | | |
| A.10.4 | Protection against malicious and mobile code | | | | | |
| A.10.4.1 | Controls against malicious code | X | X | required | | sample of servers, desktops, gateways<br>active content |

| Controls in ISO/IEC 27001:2005, Appendix 1 | | Organizational control | Technical control | System testing<br><br>*possible*<br>*recommended*<br>*required* | Visual inspection | Comment |
|---|---|---|---|---|---|---|
| A.10.4.2 | Controls against mobile code | X | X | possible | | e.g. grid-computing |
| A.10.5 | Back -up | | | | | |
| A.10.5.1 | Information back-up | X | X | recommended | | operational backup |
| A.10.6 | Network security management | | | | | |
| A.10.6.1 | Network controls | X | | | | |
| A.10.6.2 | Security of network services | X | | | | SLA's, security requirements |
| A.10.7 | Media handling | | | | | |
| A.10.7.1 | Management of removable media | X | | | | |
| A.10.7.2 | Disposal of media | X | | | | |
| A.10.7.3 | Information handling procedures | X | | | | |
| A.10.7.4 | Security of system documentation | X | | | X | |
| A.10.8 | Exchange of information | | | | | |
| A.10.8.1 | Information exchange policies and procedures | X | | | | |
| A.10.8.2 | Exchange agreements | X | | | | |
| A.10.8.3 | Physical media in transit | X | | | | |
| A.10.8.4 | Electronic messaging | X | | | | see policy re. use of e-mail for classified information |
| A.10.8.5 | Business information systems | X | | | | |
| A.10.9 | Electronic commerce services | | | | | |
| A.10.9.1 | Electronic commerce | X | | | | |
| A.10.9.2 | On-line transactions | X | X | recommended | | check: integrity, access premissions |
| A.10.9.3 | Publicly available information | X | | | | |
| A.10.10 | Monitoring | | | | | |
| A.10.10.1 | Audit logging | X | X | possible | | on-line or printed |
| A.10.10.2 | Monitoring system use | X | X | possible | | |
| A.10.10.3 | Protection of log information | X | X | possible | | |

| Controls in ISO/IEC 27001:2005, Appendix 1 | | Organizational control | Technical control | System testing<br>*possible*<br>*recommended*<br>*required* | Visual inspection | Comment |
|---|---|---|---|---|---|---|
| A.10.10.4 | Administrator and operator logs | X | | | | |
| A.10.10.5 | Fault logging | X | | | | |
| A.10.10.6 | Clock synchronization | | X | possible | | note: Kerberos needs Clock synchronization |
| A.11 | Access control | | | | | |
| A.11.1 | Business requirement for access control | | | | | |
| A.11.1.1 | Access control policy | X | | | | |
| A.11.2 | User access management | | | | | |
| A.11.2.1 | User registration | X | | | | |
| A.11.2.2 | Privilege management | X | X | possible | | internal transfer of staff |
| A.11.2.3 | User password management | X | | | | |
| A.11.2.4 | Review of user access rights | X | | | | |
| A.11.3 | User responsibilities | | | | | |
| A.11.3.1 | Password use | X | | | | User Guidelines, Policy |
| A.11.3.2 | Unattended user equipment | X | | | | User Guidelines, Policy |
| A.11.3.3 | Clear desk and clear screen policy | X | | | X | |
| A.11.4 | Network access control | | | | | |
| A.11.4.1 | Policy on use of network services | X | | | | |
| A.11.4.2 | User authentication for external connections | X | X | required | | |
| A.11.4.3 | Equipment identification in networks | | X | | | usually not implemented |
| A.11.4.4 | Remote diagnostic and configuration port protection | | X | recommended | | |
| A.11.4.5 | Segregation in networks | X | X | possible | | network diagrams: WAN, LAN, VLAN, VPN, network objects, network segments (e.g. DMZ) |
| A.11.4.6 | Network connection control | X | X | recommended | | shared networks not very common |
| A.11.4.7 | Network routing control | X | X | required | | Firewalls, Routers/Switches: Rulebase, ACL's, Access Control |

| Controls in ISO/IEC 27001:2005, Appendix 1 | | Organizational control | Technical control | System testing<br>*possible*<br>*recommended*<br>*required* | Visual inspection | Comment |
|---|---|---|---|---|---|---|
| | | | | | | Policies |
| A.11.5 | Operating system access control | | | | | |
| A.11.5.1 | Secure log-on procedures | X | X | recommended | | |
| A.11.5.2 | User identification and authentication | X | X | recommended | | |
| A.11.5.3 | Password management system | X | X | recommended | | |
| A.11.5.4 | Use of system utilities | X | X | recommended | | |
| A.11.5.5 | Session time-out | X | X | possible | X | |
| A.11.5.6 | Limitation of connection time | X | X | possible | X | |
| A.11.6 | Application and information access control | | | | | |
| A.11.6.1 | Information access restriction | X | X | required | | |
| A.11.6.2 | Sensitive system isolation | X | X | possible | | |
| A.11.7 | Mobile computing and teleworking | | | | | |
| A.11.7.1 | Mobile computing and communications | X | | | | |
| A.11.7.2 | Teleworking | X | | | | |
| A.12 | Information systems acquisition, development and maintenance | | | | | |
| A.12.1 | Security requirements of information systems | | | | | |
| A.12.1.1 | Security requirements analysis and specification | X | | | | |
| A.12.2 | Correct processing in applications | | | | | |
| A.12.2.1 | Input data validation | X | X | | | software development guidelines, SW testing |
| A.12.2.2 | Control of internal processing | X | X | | | software development guidelines, SW testing |
| A.12.2.3 | Message integrity | | X | | | usually not required/implemented |
| A.12.2.4 | Output data validation | X | X | | | software development guidelines, SW testing |
| A.12.3 | Cryptographic controls | | | | | |

| Controls in ISO/IEC 27001:2005, Appendix 1 | | Organizational control | Technical control | System testing<br><br>*possible*<br>*recommended*<br>*required* | Visual inspection | Comment |
|---|---|---|---|---|---|---|
| A.12.3.1 | Policy on the use of cryptographic controls | **X** | **X** | possible | | |
| A.12.3.2 | Key management | **X** | **X** | required | | |
| A.12.4 | Security of system files | | | | | |
| A.12.4.1 | Control of operational software | **X** | **X** | | | |
| A.12.4.2 | Protection of system test data | **X** | **X** | | **X** | |
| A.12.4.3 | Access control to program source code | **X** | **X** | recommended | | |
| A.12.5 | Security in development and support processes | | | | | |
| A.12.5.1 | Change control procedures | **X** | | | | |
| A.12.5.2 | Technical review of applications after operating system changes | **X** | | | | |
| A.12.5.3 | Restrictions on changes to software packages | **X** | | | | |
| A.12.5.4 | Information leakage | **X** | **X** | possible | | Backdoors, e.g. via debug-functionality (legal controls), unknpown services, source code inspection |
| A.12.5.5 | Outsourced software development | **X** | | | | |
| A.12.6 | Technical Vulnerability Management | | | | | |
| A.12.6.1 | Control of technical vulnerabilities | **X** | | | | |
| A.13 | Information security incident management | | | | | |
| A.13.1 | Reporting information security events and weaknesses | | | | | |
| A.13.1.1 | Reporting information security events | **X** | | | | |
| A.13.1.2 | Reporting security weaknesses | **X** | | | | |
| A.13.2 | Management of information security incidents and improvements | | | | | |
| A.13.2.1 | Responsibilities and procedures | **X** | | | | |
| A.13.2.2 | Learning from information security incidents | **X** | | | | |

| Controls in ISO/IEC 27001:2005, Appendix 1 | | Organizational control | Technical control | System testing<br>*possible*<br>*recommended*<br>*required* | Visual inspection | Comment |
|---|---|---|---|---|---|---|
| A.13.2.3 | Collection of evidence | X | | | | |
| A.14 | Business continuity management | | | | | |
| A.14.1 | Information security aspects of business continuity management | | | | | |
| A.14.1.1 | Including information security in the business continuity management process | X | | | | |
| A.14.1.2 | Business continuity and risk assessment | X | | | | |
| A.14.1.3 | Developing and implementing continuity plans including information security | X | | | X | DR-Site inspection,<br>distance of DR-site according to risk assessment and applicable legal/regulatory requirements |
| A.14.1.4 | Business continuity planning framework | X | | | | |
| A.14.1.5 | Testing maintaining and reassessing business continuity plans | X | | | | |
| A.15 | Compliance | | | | | |
| A.15.1 | Compliance with legal requirements | | | | | |
| A.15.1.1 | Identification of applicable legislation | X | | | | |
| A.15.1.2 | Intellectual property rights (IPR) | X | | | | |
| A.15.1.3 | Protection of organizational records | X | | | | |
| A.15.1.4 | Data protection and privacy of personal information | X | | | | |
| A.15.1.5 | Prevention of misuse of information processing facilities | X | | | | |
| A.15.1.6 | Regulation of cryptographic controls | X | | | | |
| A.15.2 | Compliance with security policies and standards, and technical compliance | | | | | |
| A.15.2.1 | Compliance with security policies and standards | X | | | | |
| A.15.2.2 | Technical compliance checking | X | X | | | assess process and follow-up |
| A.15.3 | Information systems audit considerations | | | | | |

| Controls in ISO/IEC 27001:2005, Appendix 1 | | Organizational control | Technical control | System testing<br>*possible*<br>*recommended*<br>*required* | Visual inspection | Comment |
|---|---|---|---|---|---|---|
| A.15.3.1 | Information systems audit controls | **X** | | | | |
| A.15.3.2 | Protection of information systems audit tools | **X** | **X** | possible | | |