INTERNATIONAL STANDARD

ISO/IEC 27006

First edition
2007-03-01

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27006:2007(E)

© ISO/IEC 2007

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2007

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2007 – All rights reserved

Not for Resale

Contents

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Principles 2

5 General requirements 2
5.1 Legal and contractual matter 2
5.2 Management of impartiality 2
5.3 Liability and financing 3

6 Structural requirements 3
6.1 Organizational structure and top management 3
6.2 Committee for safeguarding impartiality 3

7 Resource requirements 3
7.1 Competence of management and personnel 3
7.2 Personnel involved in the certification activities 4
7.3 Use of individual external auditors and external technical experts 6
7.4 Personnel records 6
7.5 Outsourcing 6

8 Information requirements 6
8.1 Publicly accessible information 6
8.2 Certification documents 6
8.3 Directory of certified clients 7
8.4 Reference to certification and use of marks 7
8.5 Confidentiality 7
8.6 Information exchange between a certification body and its clients 7

9 Process requirements 7
9.1 General requirements 7
9.2 Initial audit and certification 11
9.3 Surveillance activities 15
9.4 Recertification 16
9.5 Special audits 16
9.6 Suspending, withdrawing or reducing scope of certification 16
9.7 Appeals 17
9.8 Complaints 17
9.9 Records of applicants and clients 17

10 Management system requirements for certification bodies 17
10.1 Options 17
10.2 Option 1 – Management system requirements in accordance with ISO 9001 17
10.3 Option 2 – General management system requirements 17

Annex A (informative) **Analysis of a client organization's complexity and sector-specific aspects** 18

Annex B (informative) **Example areas of auditor competence** 21

Annex C (informative) **Audit time** 23

Annex D (informative) **Guidance for review of implemented ISO/IEC 27001:2005, Annex A controls** 29

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO and 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 technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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

ISO/IEC 27006 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

ISO/IEC 17021 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 with the objective of auditing and certifying Information Security Management Systems (ISMS) in accordance with ISO/IEC 27001:2005, some additional requirements and guidance to ISO/IEC 17021 are necessary. These are provided by this International Standard.

The text in this International Standard follows the structure of ISO/IEC 17021, and the additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021 for ISMS certification are identified by the letters “IS”.

The term “shall” is used throughout this International Standard to indicate those provisions which, reflecting the requirements of ISO/IEC 17021 and ISO/IEC 27001, are mandatory. The term “should” is used to indicate those provisions which, although they constitute guidance for the application of the requirements, are expected to be adopted by a certification body.

One aim of this International Standard is to enable accreditation bodies to more effectively harmonise their application of the standards against which they are bound to assess certification bodies. In this context, any variation from the guidance by a certification body is an exception. Such variations will only be permitted on a case-by-case basis after the certification body has demonstrated to the accreditation body that the exception meets in some equivalent way the relevant requirements clause of ISO/IEC 17021, ISO/IEC 27001 and the intent of this International Standard.

NOTE Throughout this International Standard, the terms “management system” and “system” are used interchangeably. The definition of a management system can be found in ISO 9000:2005. The management system as used in this International Standard is not to be confused with other types of system, such as IT systems.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

1 Scope

This International Standard specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.

The requirements contained in this International Standard need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in this International Standard provides additional interpretation of these requirements for any body providing ISMS certification.

NOTE This International Standard can be used as a criteria document for accreditation, peer assessment or other audit processes.

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*

ISO/IEC 19011, *Guidelines for quality and/or environmental management systems auditing*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021, ISO/IEC 27001 and the following apply.

3.1
certificate
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
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

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.4
mark
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

The principles from ISO/IEC 17021:2006, Clause 4 apply.

5 General requirements

5.1 Legal and contractual matter

The requirements from ISO/IEC 17021:2006, Clause 5.1 apply.

5.2 Management of impartiality

The requirements from ISO/IEC 17021:2006, Clause 5.2 apply. In addition, the following ISMS-specific requirements and guidance apply.

5.2.1 IS 5.2 Conflicts of interest

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 ISMS 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, certification bodies 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 describing the certification body's interpretation of the requirements of the certification audit standards;

d) activities prior to audit, solely aimed at determining readiness for certification audit; however, 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 standards or regulations other 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 ISMS audit of the client organization's ISMS subject to certification.

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.3 Liability and financing

The requirements from ISO/IEC 17021:2006, Clause 5.3 apply.

6 Structural requirements

6.1 Organizational structure and top management

The requirements from ISO/IEC 17021:2006, Clause 6.1 apply.

6.2 Committee for safeguarding impartiality

The requirements from ISO/IEC 17021:2006, Clause 6.2 apply.

7 Resource requirements

7.1 Competence of management and personnel

The requirements from ISO/IEC 17021:2006, Clause 7.1 apply. In addition, the following ISMS-specific requirements and guidance apply.

7.1.1 IS 7.1 Management competence

The essential elements of competence required to perform ISMS certification are to select, provide and manage those individuals whose skills and collective competence is appropriate to the activities to be audited and the related information security issues.

7.1.1.1 Competence analysis and contract review

The certification body shall ensure that it has 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.

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.

7.1.1.2 Resources

The management of the certification body shall have the necessary processes and 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 competence of auditors may be established by verified background experience and specific training or briefing (see also Annex B). The certification body shall be able to communicate effectively with all those clients it provides services to.

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.2 Personnel involved in the certification activities

The requirements from ISO/IEC 17021:2006, Clause 7.2 apply. In addition, the following ISMS-specific requirements and guidance apply.

7.2.1 IS 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 and complaints process.

7.2.1.1 Training of audit teams

The certification body shall have criteria for the training of audit teams that ensures

a) knowledge of the ISMS standard and other relevant 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) general knowledge of regulatory requirements relevant to ISMSs;

f) knowledge of management systems;

g) understanding of the principles of auditing based on ISO 19011;

h) knowledge of ISMS effectiveness review and 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.

7.2.1.1.1 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 within the scope of the ISMS for which certification is sought and, where relevant, with associated procedures and their potential information security risks (technical experts who are not auditors may fulfil this function);

b) have a sufficient degree of understanding of the client organization to conduct a reliable certification audit of its ISMS in managing the information security aspects of its activities, products and services;

c) have appropriate understanding of the regulatory requirements applicable to the client organization's ISMS.

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.2.1.1.2 When required, the audit team may be complemented 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 but could advise auditors on matters of technical adequacy in the context of the management system being subjected to audit. 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.

7.2.1.2 Management of the decision taking process

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

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

7.2.1.3.1 The following criteria shall be applied for each auditor in the ISMS audit team. The auditor shall

a) have an education at secondary level;

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

c) have successfully completed five days of training, the scope of which covers ISMS audits and audit management shall be considered appropriate;

d) have gained experience in the entire process of assessing information security prior to assuming responsibility for performing as an auditor. This experience should 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) have experience which is reasonably current;

f) be able to put complex operations in a broad perspective and 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.

Technical experts shall comply with criteria a), b), e) and f).

7.2.1.3.2 In addition to the requirements in 7.2.1.3.1, audit team leaders shall fulfil the following requirements, which shall be demonstrated in audits under guidance and supervision:

a) have knowledge and attributes to manage the certification audit process;

b) have been an auditor in at least three complete ISMS audits;

c) have demonstrated the capability to communicate effectively, both orally and in writing.

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.3 Use of individual external auditors and external technical experts

The requirements from ISO/IEC 17021:2006, Clause 7.3 apply. In addition, the following ISMS-specific requirements and guidance applies.

7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team

When using individual external auditors or external technical experts as part of the audit team, the certification body shall ensure that they are competent and comply with the applicable provisions of this publication and are not involved, either directly or through its employer with the design, implementation or maintenance of an ISMS or related management system(s) in such a way that impartiality could be compromised.

7.3.1.1 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 criteria in 7.2, may be part of the audit team. Technical experts shall work under the supervision of an auditor.

7.4 Personnel records

The requirements from ISO/IEC 17021:2006, Clause 7.4 apply.

7.5 Outsourcing

The requirements from ISO/IEC 17021:2006, Clause 7.5 apply.

8 Information requirements

8.1 Publicly accessible information

The requirements from ISO/IEC 17021:2006, Clause 8.1 apply. In addition, the following ISMS-specific requirements and guidance apply.

8.1.1 IS 8.1 Procedures for granting, maintaining, extending, reducing, suspending and withdrawing certification

The certification body shall require the client organization to have a documented and implemented ISMS which conforms to ISO/IEC 27001 and other documents required for certification.

The certification body shall have documented procedures 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

The requirements from ISO/IEC 17021:2006, Clause 8.2 apply. In addition, the following ISMS-specific requirements and guidance apply.

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.2.1 IS 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 and the ISMS standard ISO/IEC 27001 to which the ISMS is certified. In addition, the certificate should include a reference to the specific version of the Statement of Applicability.

8.3 Directory of certified clients

The requirements from ISO/IEC 17021:2006, Clause 8.3 apply.

8.4 Reference to certification and use of marks

The requirements from ISO/IEC 17021:2006, Clause 8.4 apply. In addition, the following ISMS-specific requirements and guidance applies.

8.4.1 IS 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 mark to indicate certification of an ISMS, the certification body should ensure that the client organization uses the specified mark only as authorised in writing by the certification body. The certification body shall not entitle the client organization to use this mark on a product, or in a way that may be interpreted as denoting product conformity.

8.5 Confidentiality

The requirements from ISO/IEC 17021:2006, Clause 8.5 apply. In addition, the following ISMS-specific requirements and guidance applies.

8.5.1 IS 8.5 Access to organizational records

Before the certification audit, the certification body shall ask the client organization to report 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 audited in the absence of these records. If the certification body concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive records, it shall advise the client organization that the certification audit cannot take place until appropriate access arrangements are granted.

8.6 Information exchange between a certification body and its clients

The requirements from ISO/IEC 17021:2006, Clause 8.6 apply.

9 Process requirements

9.1 General requirements

The requirements from ISO/IEC 17021:2006, Clause 9.1 apply. In addition, the following ISMS-specific requirements and guidance apply.

9.1.1 IS 9.1.1 General ISMS audit requirements

9.1.1.1 Certification audit criteria

The criteria against which the ISMS of a client are audited shall be those outlined in the ISMS standard ISO/IEC 27001 and other documents required for certification relevant to the function performed. If an

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

explanation is required as to the application of these documents to a specific certification programme, then such an explanation shall be given by a relevant and impartial committee or persons possessing the necessary technical competence and published by the certification body.

9.1.1.2 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 ISMSs and the procedures for auditing and certifying the client organization's ISMS.

9.1.1.3 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.

9.1.2 IS 9.1.2 Scope of certification

The audit team shall audit 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 certification body shall confirm, in the scope of their ISMS, that client organizations address the requirements stated in Clause 1.2 of ISO/IEC 27001:2005.

Certification bodies shall ensure that the client organization's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the 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. IT systems, databases and telecommunication systems) with other organizations.

9.1.3 IS 9.1.3 Audit time

Certification bodies shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or recertification audit. The time allocated should be based on factors such as

a) the size of the ISMS scope (e.g. number of information systems used, number of employees);

b) complexity of the ISMS (e.g. criticality of information systems, risk situation of the ISMS), see also Annex A;

c) the type(s) of business performed within scope of the ISMS;

d) extent and diversity of technology utilized in the implementation of the various components of the ISMS (such as the implemented controls, documentation and/or process control, corrective/preventive action, etc);

e) number of sites;

f) previously demonstrated performance of the ISMS;

g) extent of outsourcing and third party arrangements used within the scope of the ISMS;

h) the standards and regulations which apply to the certification.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C provides guidance on Audit Time. The certification body shall be prepared to substantiate or justify the amount of time used in any initial audit, surveillance audits and recertification audit.

9.1.4 IS 9.1.4 Multiple sites

9.1.4.1 Multiple site sampling decisions in the area of ISMS certification are more complex than the same decisions are for quality management systems. Where a client organization has a number of sites meeting the criteria from a) to c) below, certification bodies may consider using a sample-based approach to multiple-site certification audit:

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 programme;

c) all sites are included within the client organisation's ISMS management review programme.

9.1.4.2 The certification body wishing to use a sample-based approach shall have procedures in place to ensure the following.

a) The initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined.

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

   1) the results of internal audits of head office and the sites,

   2) the results of management review,

   3) variations in the size of the sites,

   4) variations in the business purpose of the sites,

   5) complexity of the ISMS,

   6) complexity of the information systems at the different sites,

   7) variations in working practices,

   8) variations in activities undertaken,

   9) potential interaction with critical information systems or information systems processing sensitive information,

   10) any differing legal requirements.

c) A representative sample is selected from all sites within the scope of the client organization's ISMS; this selection should be based upon judgmental choice to reflect the factors presented in item b) above as well as a random element.

d) Every site included in the ISMS which is subject to significant risks is audited by the certification body prior to certification.

e) The surveillance programme has been designed in the light of the above requirements and covers all sites of the client organization or within the scope of the ISMS certification within a reasonable time.

f) In the case of a nonconformity being observed, either at the head office or at a single site, the corrective action procedure applies to the head office and all sites covered by the certificate.

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The audit described in IS 9.1.5 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.

9.1.5 IS 9.1.5 Audit Methodology

The certification body shall have procedures, which require the client organization to be able to demonstrate that the internal ISMS audits are 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 shall focus on establishing that a client organization's ISMS meets the requirements of the ISO/IEC 27001 standard and the policies and objectives of the client organization.

The audit plan should identify the network-assisted auditing techniques that will be utilized during the audit, as appropriate.

NOTE Network assisted auditing techniques may include, for example, teleconferencing, web meeting, interactive web-based communications and remote electronic access to the ISMS documentation and/or ISMS processes. The focus of such techniques should be to enhance audit effectiveness and efficiency, and should support the integrity of the audit process.

9.1.6 IS 9.1.6 Certification Audit Report

9.1.6.1 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 client organization's premises at which the audit team provides

   1) a written or oral indication regarding the conformity of the client organization's ISMS with the particular certification requirements,

   2) an opportunity for the client organization to ask questions about the findings and their basis;

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

9.1.6.2 The audit report should provide the following information:

a) an account of the audit including a summary of the document review;

b) an account of the certification audit of the client organization's information security risk analysis;

c) total audit time used and detailed specification of time spent on document review, assessment of risk analysis, on-site audit, and audit reporting;

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

9.1.6.3 The audit report of findings provided to the certification body shall be of sufficient detail to facilitate and support a certification decision and shall contain

a) areas covered by the audit (e.g. the certification requirements and the sites that were audited), including significant audit trails followed and audit methodologies utilized (see IS 9.1.5);

b) observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities);

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

c) details of any nonconformities identified, supported by objective evidence and a reference of these nonconformities to the requirements of the ISMS standard ISO/IEC 27001 or other documents required for certification;

d) comments on the conformity of the client organization's ISMS with the certification requirements with a clear statement of nonconformity, a reference to the version of the Statement of Applicability, and, where applicable, any useful comparison with the results of previous certification audits of the client organization.

Completed questionnaires, checklists, observations, logs, or auditor notes might form an integral part of the audit report. If these methods are used, these documents shall be submitted to the certification body as evidence to support the certification decision. Information about the samples evaluated during the audit should be included in the audit report, or in other certification documentation.

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 17021:2006, Clause 9.1.10, the report should cover

— the degree of reliance that can be placed on the internal ISMS audits and management reviews;

— a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS;

— the audit team's recommendation as to whether the client organization's ISMS should be certified or not, with information to substantiate this recommendation.

9.2 Initial audit and certification

The requirements from ISO/IEC 17021:2006, Clause 9.2 apply. In addition, the following ISMS-specific requirements and guidance apply.

9.2.1 IS 9.2.1 Audit team competence

The following requirements apply to certification assessment, in addition to the requirements that are listed in Clause 7.2. For surveillance activities only those requirements which are relevant to the scheduled surveillance activity apply.

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

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

   1) managing the team,

   2) management systems and process applicable to ISMS,

   3) knowledge of the legislative and regulatory requirements in the particular information security field,

   4) identifying information security related threats and incident trends,

   5) identifying the vulnerabilities of the client organization and understanding the likelihood of their exploitation, their impact and their mitigation and control,

   6) knowledge of ISMS controls and their implementation,

   7) knowledge of ISMS effectiveness review and measurement of controls,

   8) related and/or relevant ISMS standards, industry best practices, security policies and procedures,

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9) knowledge of incident handling methods and business continuity,

10) knowledge about tangible and intangible information assets and impact analysis,

11) knowledge of the current technology where security might be relevant or an issue,

12) knowledge of risk management processes and methods.

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

c) The audit team shall have 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).

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

9.2.1.1 IS 9.2.1.1 Demonstration of auditor competence

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.

9.2.2 IS 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 client prior to the onsite certification audit:

a) general information concerning the ISMS and the activities it covers;

b) a copy of the ISMS documentation required in ISO/IEC 27001:2005, Clause 4.3.1 and, where required, associated documentation.

9.2.3 IS 9.2.3 Initial certification audit

9.2.3.1 IS 9.2.3.1 Stage 1 audit

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 objective of the stage 1 audit is to provide a focus for planning the stage 2 audit 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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The stage 1 audit 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 shall be completed prior to the commencement of the stage 2 audit.

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

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

9.2.3.2 IS 9.2.3.2 Stage 2 audit

9.2.3.2.1 The stage 2 audit always takes place at the site(s) of the client organization. On the basis of findings documented in the stage 1 audit report, the certification body drafts an audit plan for the conduct of the stage 2 audit. The objectives of the stage 2 audit are

a) to confirm that the client organization adheres to its own policies, objectives and procedures;

b) to confirm that the ISMS conforms to all the requirements of the normative ISMS standard ISO/IEC 27001 and is achieving the client organization's policy objectives.

9.2.3.2.2 To do this, the audit shall focus on the client organization's

a) assessment of information security related risks, and that the assessments produce comparable and reproducible results;

b) documentation requirements listed in Clause 4.3.1 of ISO/IEC 27001:2005;

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 D), taking into account the organization's measurements of effectiveness of controls [see d) above], 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.

9.2.3.3 IS 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

a) require the client organization to demonstrate that the analysis of security related threats is relevant and adequate for the operation of the client organization;

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

NOTE The client organization is responsible for defining criteria by which information security related risks of the client organization are identified as significant, and to develop procedure(s) for doing this.

b) 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 shall also 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.

9.2.3.3.1 Legal and regulatory compliance

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

9.2.3.3.2 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.

9.2.3.3.3 Combining management system audits

A certification body may offer other management system certification linked with the 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 shall appear clearly, and be readily identifiable, in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits.

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

9.2.4 IS 9.2.4 Information for granting initial certification

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

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 the information required in IS 9.1.6.

9.2.5 IS 9.2.5 Certification decision

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.

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. This decision shall be based upon the findings and certification recommendation of the audit team as provided in their certification audit report (see IS 9.1.6) and any other relevant information available to the certification body.

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 ISMS audit and one management review of the client organization's ISMS shall have taken place. The certification body may specify such 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 and internal ISMS audit processes.

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

9.3 Surveillance activities

The requirements from ISO/IEC 17021:2006, Clause 9.3 apply. In addition, the following ISMS-specific requirements and guidance apply.

9.3.1 IS 9.3 Surveillance audits

9.3.1.1 Surveillance 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 programs should normally cover

a) the system maintenance elements which are internal ISMS audit, management review and preventive and corrective action;

b) communications from external parties as required by the ISMS standard ISO/IEC 27001 and other documents required for certification;

c) changes to the documented system;

d) areas subject to change;

e) selected elements of ISO/IEC 27001;

f) other selected areas as appropriate.

9.3.1.2 As a minimum, surveillance by the certification body shall 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.

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.3.1.3 Surveillance by the certification body should at least cover the points required for surveillance audit 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 shall clearly indicate the aspects relevant to each management system.

d) The certification body is required to supervise the appropriate use of the certificate.

During surveillance audits, certification bodies shall check the records of appeals and complaints 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.

A surveillance report shall 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.

9.4 Recertification

The requirements from ISO/IEC 17021:2006, Clause 9.4 apply. In addition, the following ISMS-specific requirements and guidance apply.

9.4.1 IS 9.4 Recertification audits

Recertification audit procedures shall be consistent with those concerning the certification audit of the client organization's ISMS as described in this International Standard.

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 the scope of certification shall be reduced, or the certificate 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 of the client organization meeting specified requirements.

9.5 Special audits

The requirements from ISO/IEC 17021:2006, Clause 9.5 apply. In addition, the following ISMS-specific requirements and guidance apply.

9.5.1 IS 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.

9.6 Suspending, withdrawing or reducing scope of certification

The requirements from ISO/IEC 17021:2006, Clause 9.6 apply.

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.7 Appeals

The requirements from ISO/IEC 17021:2006, Clause 9.7 apply.

9.8 Complaints

The requirements from ISO/IEC 17021:2006, Clause 9.8 apply. In addition, the following ISMS-specific requirements and guidance apply.

9.8.1 IS 9.8 Complaints

Complaints represent a source of information as to possible nonconformity. The certification body should require the certified client organization that, on receipt of a complaint, the certified client organization should establish, and where appropriate report on, the cause of the complaint, 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

a) notification to appropriate authorities if required by regulation;

b) restoring conformity;

c) preventing recurrence;

d) evaluating and mitigating any adverse security incidents and their associated impacts;

e) ensuring satisfactory interaction with other components of the ISMS;

f) 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 of applicants and clients

The requirements from ISO/IEC 17021:2006, Clause 9.9 apply.

10 Management system requirements for certification bodies

10.1 Options

The requirements from ISO/IEC 17021:2006, Clause 10.1 apply.

10.2 Option 1 – Management system requirements in accordance with ISO 9001

The requirements from ISO/IEC 17021:2006, Clause 10.2 apply.

10.3 Option 2 – General management system requirements

The requirements from ISO/IEC 17021:2006, Clause 10.3 apply. In addition, the following ISMS-specific requirements and guidance apply.

10.3.1 IS 10.3 ISMS implementation

It is recommended that certification bodies implement an ISMS in accordance with ISO/IEC 27001.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(informative)

Analysis of a client organization's complexity and sector-specific aspects

A.1 Organization's risk potential

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

The complexity category assigned to an ISMS scope can then be used to decide

a) the auditors' competence requirements for the ISMS audit (an example of which is given in Annex B);

b) the audit time requirements for the ISMS audit (an example of which is given in Annex C).

Table A.1 is a general indication of the possible factors to be considered when determining an ISMS scope's complexity. It might need to be adapted to specific circumstances or have any special factors included, as seen appropriate.

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

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table A.1 — Criteria for ISMS Scope Complexity

Complexity Factor	Category			Significance
	High	Medium	Low	
Number of employees + contractor staff	≥1,000	≥200	<200	• Scale of ISMS implementation • Management information system • Production management-related systems • Sales/distribution/general service-related systems • Information technology/information services and related systems • Construction/ship-building/plant engineering-related systems
Number of users	≥1million	≥200,000	< 200,000	• Financial systems • Governments, Schools, Medicals/hospitals systems
Number of sites	≥5	≥2	1	• Scale of ISMS implementation • Physical and environmental security (ISO/IEC 27001:2005, A.9)
Number of servers	≥100	≥10	<10	• Scale of ISMS implementation • Physical and environmental security (A.9) • Access control (ISO/IEC 27001:2005, A.11) • Telecommunications and operation management (ISO/IEC 27001:2005, A.10)
Number of workstations + PC + laptops	≥300	≥50	<50	• Access control (ISO/IEC 27001:2005, A.11)
Number of application development and maintenance staff	≥100	≥ 20	< 20	• Information systems acquisition, development and maintenance (ISO/IEC 27001:2005, A.12)
Network & encryption technology	External / internet connection with encryption / digital signature / PKI requirements	External / internet connection with use of encryption in built in standard facilities and without digital signature / PKI requirements	External / internet connection without encryption / digital signature / PKI requirements	• Telecommunications and operation management (ISO/IEC 27001:2005, A.10) • Access control (ISO/IEC 27001:2005, 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 (ISO/IEC 27001:2005, A.15)
Applicability of sector-specific risk *(refer to A.2 for examples of sector-specific categories of information security risk)*	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 • Laws and guidelines (ISO/IEC 27001:2005, A.15)

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.2 Sector-specific categories of information security risk

Risks to information may be specific to the type of information considered or the sector in which an organisation operates. The following examples illustrate different categories of risk.

Specific categories applicable to all organisations:

- salaries, pensions, health and safety, organizational records, internal and interdepartmental information, etc.;
- any other personally identifiable information;
- any other commercially sensitive/critical information, such as research & development information, design information, customers details, financial results and forecasts, business plans, intellectual property rights, manufacturing processes, etc.

Government sensitive/critical information:

- public information;
- e-government applications;
- information held about citizens (e.g. health, benefit, taxes, records, etc.);
- information handled by suppliers and manufacturers of government, such as ICT designs, facilities, products, services, etc.

Specific categories applicable to classes of organisation:

- corporate governance – listed companies (possibly also other large entities).

Specific categories applicable to business sectors:

- healthcare;
- education;
- aerospace;
- telecoms;
- financial services;
- charities and non-profit organizations.

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(informative)

Example areas of auditor competence

B.1 General competence considerations

There are several ways by which an auditor can prove their knowledge and experience. Knowledge and experience can be demonstrated, for example, by using recognised qualifications. Registration, e.g. under IRCA or any other recognised form of auditor registration, can also be used to demonstrate the required knowledge and experience. The required competence level for the audit team should be established, corresponding with the organization's industry/technological field and complexity factor.

B.2 Specific competence considerations

B.2.1 Knowledge of ISO/IEC 27001:2005, Annex A controls

The following describes the typical knowledge in relation to ISMS auditing. In addition to the control areas from ISO/IEC 27001:2005, Annex A, which are listed in the following table, auditors should also be aware of the other standards in the 27000 family of standards.

Knowledge and experience of policies and business requirements for information security	Security policy
General knowledge and experience of business processes, practices and organizational structures	Organization of information security
Knowledge of asset valuation, inventories, classifications, and acceptable use policies	Asset management
General knowledge and experience of the processes and procedures used by human resources departments	Human resources security
Knowledge of physical and environmental security	Physical and environmental security
Up-to-date knowledge and experience of the standards, processes, techniques and methods used for information security, including management measures as well as an appropriate level of technical expertise. This includes current knowledge of some of the common business practices.	Communications and 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 procedures for business continuity	Business continuity management
Up-to-date knowledge of business contractual issues, and common laws and regulations related to ISMS	Compliance

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.2.2 Typical knowledge related to ISMS

Auditors should have knowledge and understanding of the following auditing and ISMS subjects:

- audit programming and planning,
- audit type and methodologies,
- audit risk,
- information security processes analysis,
- Deming cycle (PDCA) for continual improvement,
- internal auditing for information security.

Auditors should have knowledge and understanding of the following regulatory requirements:

- intellectual property,
- content, protection and retention of organizational records,
- data protection and privacy,
- regulation of cryptographic controls,
- 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,
- international and national sector-specific requirements (e.g. banking).

Auditors should have knowledge and understanding of the following management requirements:

- treatment of information security risks,
- ICT outsourcing security risks,
- supply chain information security risks.

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C
(informative)

Audit time

C.1 Introduction

This annex contains further information related to Clauses 9.1, 9.2, 9.3 and 9.4 of ISO/IEC 17021:2006. It should also be read in conjunction with Clauses IS.9.1.2, IS 9.1.3, IS 9.1.5, IS 9.1.6, IS 9.2.3.1, IS 9.2.3.2 and IS 9.2.3.3 of this International Standard. This annex provides guidance for a certification body on the development of its own procedures for determining the amount of time required for the certification of client organizations' ISMS scopes of differing sizes and complexity over a broad spectrum of activities.

Certification bodies need to identify the amount of auditor time to be spent on initial certification, surveillance and recertification for each client and certified ISMS. Using this annex at the audit-planning phase can lead to a consistent approach to the determination of appropriate auditor time. At the same time, the guidance given in this annex allows for flexibility in the light of what is found during the course of the audit, especially during the stage 1 audit and the complexity of the ISMS scope considered.

C.2 Procedure to determine audit time

Experience has shown that the scope of the ISMS, and there the number of employees (as in the auditor time chart in C.3 below), the size, characteristics, complexity and significance of potential information security risks (as explained in more detail below) will govern the amount of time taken for any given ISMS audits. Clause IS 9.1.3, and also Clauses IS 9.2.3.1, IS 9.2.3.2 and IS 9.2.3.3 list criteria, which should be considered when establishing the amount of auditor time needed. These and other factors need to be examined during the certification body's contract review process for their potential impact on the amount of auditor time to be allocated.

It is important to note that all these factors should be taken into account when determining the audit time, and that the auditor time chart in C.3 below cannot be used in isolation. The following examples illustrate factors that can influence the audit time and elaborates on the list of factors given in Clause IS 9.1.3:

- factors related to the size of the ISMS scope (e.g. number of information systems used, volume of information processed, number of users, number of privileged users, number of IT platforms, number of networks, and their size);

- factors related to the complexity of the ISMS (e.g. criticality of information systems, risk situation of the ISMS, volumes and types of sensitive and critical information handled and processed, number and types of electronic transactions, number and size of any development projects, extent of remote working taking place, extent of the ISMS documentation);

- the type(s) of business performed within scope of the ISMS, and the security, legal, regulatory, contractual and business requirements related to these types of business;

- extent and diversity of technology utilized in the implementation of the various components of the ISMS (such as the implemented controls, documentation and/or process control, corrective/preventive action, information systems, IT systems, networks, e.g. whether these are fixed, mobile, wireless, external, internal);

- number of sites within the ISMS scope, how similar or different these sites are, and whether all of the sites or a sample will be audited;

- previously demonstrated performance of the ISMS;

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- extent of outsourcing and third party arrangements used within the scope of the ISMS and dependency on these services;

- the standards, legislation and regulations which apply to the certification, and any sector-specific requirements that might apply.

The certification of an ISMS usually consumes more time than certification of a quality management system or an environmental management system, due to increased requirements on an information security management system through the specific demands of an ISMS, such as the ISMS policy, risk management, and the ISMS control objectives and controls. The certification body is required to

a) audit the soundness and consistency of the method by which the client organization determines the significance of its information security risks and impacts;

b) confirm that the system designed to achieve compliance (with all relevant legislation and other requirements which apply to the ISMS) is capable to do so and that this system is implemented and maintained;

c) confirm that the control objectives and controls have been correctly selected and implemented, that their effectiveness is measured, and that the process for achieving “prevention of and appropriate response to security failures” is sound and adhered to;

d) confirm that the document requirements of the client organization’s ISMS are fulfilled;

e) react to increased demands arising from the stage 1 audit.

C.3 Auditor time chart

C.3.1 General

The auditor time chart provided below sets out an average number of initial audit days (here and in the following, this number includes the days for the stage 1 audit and the stage 2 audit), which experience has shown to be appropriate for an ISMS scope with a given number of employees. Experience has also demonstrated that for ISMS scopes of a similar size, some will need more time and some less.

The variation of time spent on each certification depends on a number of factors including the size, scope of the audit, logistics, complexity of the organization and its state of preparedness for audit (see also C.2 above). These and other factors need to be examined during the certification body’s contract review process for their potential impact on the amount of auditor time to be allocated. Therefore the auditor time chart cannot be used in isolation.

The auditor time chart below provides the framework that could be used for audit planning by identifying a starting point based on the total number of employees for all shifts, and adjusting this based on the significant factors applying to the ISMS scope to be audited and attributing to each factor an additive or subtractive weighting to modify the base figure. The terms used in this chart are explained in C.3.2 below.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Auditor Time Chart

Number of Employees	QMS Auditor Time for Initial Audit (auditor days)	EMS Auditor Time for Initial Audit(auditor days)	ISMS Auditor Time for Initial Audit (auditor days)	Additive and Subtractive Factors	Total Auditor Time
1 ~ 10	2	3	5	See Annex C.2	
11 ~ 25	3		7	See Annex C.2	
26 ~ 45	4	6	8.5	See Annex C.2	
46 ~ 65	5		10	See Annex C.2	
66 ~ 85	6		11	See Annex C.2	
86 ~ 125	7	8	12	See Annex C.2	
126 ~ 175	8		13	See Annex C.2	
176 ~ 275	9		14	See Annex C.2	
276 ~ 425	10		15	See Annex C.2	
426 ~ 625	11	12	16.5	See Annex C.2	
626 ~ 875	12		17.5	See Annex C.2	
876 ~ 1,175	13		18.5	See Annex C.2	
1,176 ~ 1,550	14		19.5	See Annex C.2	
1,551 ~ 2,025	15	18	21	See Annex C.2	
2,026 ~ 2,675	16		22	See Annex C.2	
2,676 ~ 3,450	17		23	See Annex C.2	
3,451 ~ 4,350	18		24	See Annex C.2	
4,351 ~ 5,450	19		25	See Annex C.2	
5,451 ~ 6,800	20		26	See Annex C.2	
6,801 ~ 8,500	21		27	See Annex C.2	
8,501 ~ 10,700	22		28	See Annex C.2	
>10,700	Follow progression above		Follow progression above	See Annex C.2	

C.3.2 Explanation of terms

“Employees” as referenced in the auditor time chart refers to all individuals whose work activities relate to the scope of the ISMS. The total number of employees for all shifts is the starting point for determination of audit time.

The effective number of employees includes non-permanent (seasonal, temporary, and subcontracted) staff that will be present at the time of the audit. A certification body should agree with the organization to be audited the timing of the audit which will best demonstrate the full scope of the organization. The consideration could include season, month, day/date and shift as appropriate.

Part-time employees should be treated as full-time-equivalent employees. This determination will depend upon the number of hours worked as compared with a full-time employee.

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

"Auditor time" includes the time spent by an auditor or audit team in stage 1 audit, stage 2 audit and planning (including off-site document review, if appropriate); interfacing with organization, personnel, records, documentation and process; and report writing. It is expected that the "Auditor time" involved in such planning and report writing combined should not typically reduce the total on-site "auditor time" to less than 70 % of the time shown in the auditor time chart. Where additional time is required for planning and/or report writing, this will not be justification for reducing on-site auditor time. Auditor travel time is not included in this calculation, and is additional to the Auditor time referenced in the chart.

NOTE 1 70 % is a factor based on experience of ISMS audits.

If remote auditing techniques such as interactive web-based collaboration, web meetings, teleconferences and/or electronic verification of the organization's processes are utilized to interface with the organization, these activities should be identified in the audit plan (see IS 9.1.5), and may be considered as partially contributing to the total "on-site auditor time".

If the certification body plans an audit plan for which the remote auditing activities represent more than 30 % of the planned on-site auditor time, the certification body should justify the audit plan and obtain specific approval from the accreditation body prior to its implementation.

NOTE 2 On-site auditor time refers to the on-site auditor time allocated for individual sites. Electronic audits of remote sites are considered to be remote audits, even if the electronic audits are physically carried out on the organization's premises.

"Auditor time" as referenced in the chart is stated in terms of "Auditor Days" spent on the audit. An "Auditor Day" is typically a full normal working day.

For the initial certification audit cycle, surveillance time for a given organization should be proportional to the time spent at initial audit with the total amount of time spent annually on surveillance being about 1/3 of the time spent on the initial audit. The planned surveillance time should be reviewed from time-to-time to account for changes in the organization, system maturity, etc., and at least at the time of re-certification audit.

The total amount of time spent performing the re-certification audit will depend upon the findings of the review as defined in Clause IS 9.1.6 of this International Standard and 9.4 of ISO/IEC 17021:2006. The amount of time spent at re-certification audit should be proportional to the time that would be spent at initial certification audit of the same organization and should be about 2/3 of the time that would be required for initial certification audit of the same organization at the time that it is to be audited for re-certification. Re-certification audit time is spent as the above and beyond the routine surveillance time, but, when re-certification audit is carried out at the same time as a planned routine Surveillance visit, the re-certification audit will suffice to meet the requirement for Surveillance as well. Regardless of what conclusion is made, the guidance in IS 9.1.2 applies.

Once the general starting point for determining the required auditor time has been made for the typical ISMS scope with the number of employees indicated, some adjustments need to be considered to account for the differences that could affect the actual auditor time required to perform an effective audit for the specific ISMS to be audited in addition to those listed in C.2.

Example factors requiring additional auditor time could be

- complicated logistics involving more than one building or location in the scope of the ISMS;
- staff speaking in more than one language (requiring interpreter(s) or preventing individual auditors from working independently);
- high degree of regulation;
- ISMS covers highly complex processes or relatively high number or unique activities;
- processes involve a combination of hardware, software, process, and service;
- activities that require visiting temporary sites to confirm the activities of the permanent sites(s) whose management system is subject to certification (see Note 3 below).

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Example factors permitting less auditor time could be

- no/low risk product/processes;
- prior knowledge of the organization (for example, if the organization has already been certified to another standard by the same certification body);
- client preparedness for certification (for example, already certified or recognized by another 3rd party scheme);
- processes involve a single general activity (e.g. service only);
- maturity of the management system in place;
- high percentage of employees performing the same simple tasks.

NOTE 3 In situations where the certification client or certified organization provides their product(s) or service at temporary sites it is important that evaluations of such sites are incorporated into the certification audit and surveillance programs.

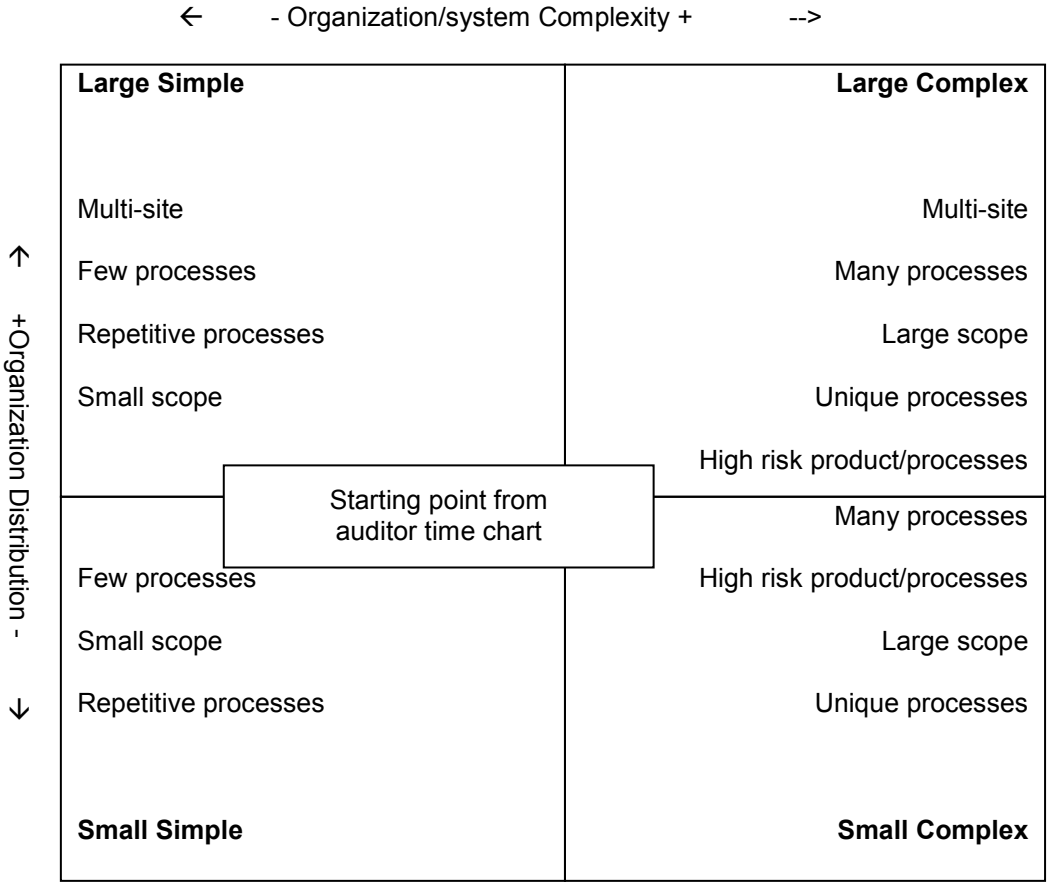
A temporary site is a location other than the sites/locations identified in the certification document where activities, within the scope of certification, are implemented for a defined period of time. These sites could range from major project management sites to minor service/installation sites. The need to visit such sites and the extent of sampling should be based on an evaluation of the risks of the failure of a product or service to meet needs/expectations due to system nonconformity. The sample of sites selected should represent the range of the organization's competency needs and service variations having given consideration to sizes and types of activities, and the various stages of projects in progress.

All attributes of the ISMS scope, processes, and products/services should be considered and a fair adjustment made for those factors that could justify more or less auditor time for an effective audit. Additive factors may be off-site by subtractive factors. In all cases where adjustments are made to the time provided in the auditor time table, sufficient evidence and records shall be maintained to justify the variation.

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The following graphic illustrates the potential interaction of additive and subtractive Factors on the Auditor Time found in the chart above.



© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex D
(informative)

Guidance for review of implemented ISO/IEC 27001:2005, Annex A controls

D.1 Purpose

This annex provides guidance for the review of the implementation of controls listed in ISO/IEC 27001:2005, Annex A, and the gathering of audit evidence as to their performance during the initial audit and subsequent surveillance visits. The implementation of all controls selected by the client organization for the ISMS (as per the Statement of Applicability) needs to be reviewed during stage 2 of the initial audit and during surveillance or recertification activities.

The audit evidence that the certification body collects needs to be sufficient to draw a conclusion as to whether the controls are effective. How a control is expected to perform will be specified in procedures or policies of the client organization stated in or referenced from the Statement of Applicability. Obviously those controls outside the scope of the ISMS will not be audited.

D.1.1 Audit evidence

The best quality audit evidence is gathered from observation by the auditor (e.g. that a locked door is locked, people do sign confidentiality agreements, the asset register exists and contains assets observed, system settings are adequate, etc). Evidence can be gathered from seeing the results of performance of a control (e.g. printouts of access rights given to people signed by the correct authorizing official, records of incident resolution, processing authorities signed by the correct authorizing official, minutes of management (or other) meetings etc.). Evidence can be the result of direct testing (or re-performance) of controls by the auditor (e.g. attempts to perform tasks said to be prohibited by the controls, determination whether software to protect against malicious code is installed and up-to-date on machines, access rights granted (after checking to authorities), etc.). Evidence can be gathered by interviewing employees/contractors about processes and controls and determining whether this is factually correct.

D.2 How to use Table D.1

D.2.1 Columns “Organizational control” and “Technical control”

An “X” in the respective column indicates whether the control is an organizational or a technical control. As some controls are both organizational and technical, entries are in both columns for such controls.

Evidence of the performance of organizational controls can be gathered through review of the records of performance of controls, interviews, observation and physical inspection. Evidence of the performance of technical controls can often be gathered through system testing (see below) or through use of specialized audit/reporting tools.

D.2.2 Column “System testing”

“System testing” means direct review of systems (e.g. review of system settings or configuration). The auditor’s questions could be answered at the system console or by evaluation of the results of testing tools. If the client organization 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 client organization (or their sub-contractors) can be reviewed.

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

There are two categories for the review of technical controls:

- "possible": system testing is possible for the evaluation of control implementation, but usually not necessary;
- "recommended": system testing is usually necessary.

D.2.3 Column "Visual inspection"

"Visual inspection" means that these controls usually require a visual inspection at the location to evaluate their effectiveness. This means that it is not sufficient to review the respective documentation on paper or through interviews – the auditor needs to verify the control at the location where it is implemented.

D.2.4 Column "Audit review guidance"

Where it might be helpful to have guidance for the audit of a particular control, the "Comments" column provides possible focus areas for the evaluation of the control, as further guidance for the auditor.

Table D.1 — Classification of controls

Controls in ISO/IEC 27001:2005, Annex A		Organ-izational control	Technical control	System testing	Visual inspec-tion	Audit review guidance
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				management review minutes
A.6	Organization of information security					
A.6.1	Internal organization					
A.6.1.1	Management commitment to information security	X				management meeting minutes
A.6.1.2	Information security co-ordination	X				management meeting minutes
A.6.1.3	Allocation of information security responsibilities	X				
A.6.1.4	Authorization process for information processing facilities	X				
A.6.1.5	Confidentiality agreements	X				sample some copies from files
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				read the reports
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				test some contract conditions

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table D.1 (*continued*)

Controls in ISO/IEC 27001:2005, Annex A		Organ-izational control	Technical control	System testing	Visual inspec-tion	Audit review guidance
A.7	Asset management					
A.7.1	Responsibility for assets					
A.7.1.1	Inventory of assets	X				identify the assets
A.7.1.2	Ownership of assets	X				
A.7.1.3	Acceptable use of assets	X				
A.7.2	Information classification					
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					sample some HR files
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				ask staff if they are aware of specific things they should be aware of
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 records
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	
A.9.2	Equipment security					
A.9.2.1	Equipment siting and protection	X	X	possible	X	
A.9.2.2	Supporting utilities	X	X	possible	X	
A.9.2.3	Cabling security	X			X	
A.9.2.4	Equipment maintenance	X				

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table D.1 (*continued*)

Controls in ISO/IEC 27001:2005, Annex A		Organ-izational control	Technical control	System testing	Visual inspec-tion	Audit review guidance
A.9.2.5	Security of equipment off premises	X	X	possible		portable device encryption
A.9.2.6	Secure disposal or re-use of equipment	X	X	possible	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	X	possible		
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	X	possible		
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	recommended		sample of servers, desktops, gateways
A.10.4.2	Controls against mobile code	X	X	possible		
A.10.5	Back -up					
A.10.5.1	Information back-up	X	X	recommended		try a recovery
A.10.6	Network security management					
A.10.6.1	Network controls	X	X	possible		
A.10.6.2	Security of network services	X				SLA's, security features
A.10.7	Media handling					
A.10.7.1	Management of removable media	X	X	possible		
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	possible	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	X	possible		encryption or physical protection
A.10.8.4	Electronic messaging	X	X	possible		confirm sample messages conform to policy/procedures
A.10.8.5	Business information systems	X				

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table D.1 (*continued*)

Controls in ISO/IEC 27001:2005, Annex A		Organ-izational control	Technical control	System testing	Visual inspec-tion	Audit review guidance
A.10.9	Electronic commerce services					
A.10.9.1	Electronic commerce	X	X	possible		
A.10.9.2	On-line transactions	X	X	recommended		check: integrity, access authorization
A.10.9.3	Publicly available information	X	X	possible		
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		
A.10.10.4	Administrator and operator logs	X	X	possible		
A.10.10.5	Fault logging	X				
A.10.10.6	Clock synchronization		X	possible		
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				sample employees/contractors to authorizations for all access rights to all systems
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				verify guidelines/policy in place for users
A.11.3.2	Unattended user equipment	X				verify guidelines/policy in place for users
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	recommended		
A.11.4.3	Equipment identification in networks		X			
A.11.4.4	Remote diagnostic and configuration port protection		X	recommended		

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table D.1 (*continued*)

Controls in ISO/IEC 27001:2005, Annex A	Organ-izational control	Technical control	System testing	Visual inspec-tion	Audit review guidance
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	recommended		Firewalls, Routers/Switches: Rule base, ACL's, Access Control 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	recommended		
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	X	possible		
A.11.7.2 Teleworking	X	X	possible		
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	recommended		software development guidelines, SW testing; confirm in sample business applications that controls required by the users exist in practice
A.12.2.2 Control of internal processing	X	X	possible		software development guidelines, SW testing; confirm in sample business applications that controls required by the users exist in practice
A.12.2.3 Message integrity		X	possible		
A.12.2.4 Output data validation	X	X	possible		software development guidelines, SW testing; confirm in sample business applications that controls required by the users exist in practice

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table D.1 (*continued*)

Controls in ISO/IEC 27001:2005, Annex A		Organ-izational control	Technical control	System testing	Visual inspec-tion	Audit review guidance
A.12.3	Cryptographic controls					
A.12.3.1	Policy on the use of cryptographic controls	X	X	possible		also check implementation of policy where appropriate
A.12.3.2	Key management	X	X	recommended		
A.12.4	Security of system files					
A.12.4.1	Control of operational software	X	X	possible		
A.12.4.2	Protection of system test data	X	X	possible	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		unknown services
A.12.5.5	Outsourced software development	X				
A.12.6	Technical Vulnerability Management					
A.12.6.1	Control of technical vulnerabilities	X	X	recommended		patch distribution
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				
A.13.2.3	Collection of evidence	X				
A.14	Business continuity management					
A.14.1	Information security aspects of business continuity management					management review minutes
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	possible	X	DR-Site inspection, distance of DR-site according to risk assessment and applicable legal/regulatory requirements

© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table D.1 (*continued*)

Controls in ISO/IEC 27001:2005, Annex A		Organ-izational control	Technical control	System testing	Visual inspec-tion	Audit review guidance
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**	**X**	possible		
A.15.1.4	Data protection and privacy of personal information	**X**	**X**	possible		
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					
A.15.3.1	Information systems audit controls	**X**				
A.15.3.2	Protection of information systems audit tools	**X**	**X**	possible		

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 36 pages

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale