ISO/IEC JTC 1/SC 27 **N6222**

ISO/IEC JTC 1/SC 27/WG 1 **N16222**

REPLACES: N5963

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	text for Working Draft
TITLE:	**Text for ISO/IEC 1st WD 27007 -- Information technology -- Security techniques -- Guidelines for information security management systems auditing**
SOURCE:	Project Editor (A. Plate)
DATE :	2007-11-02
PROJECT:	27007
STATUS:	In accordance with resolution 6 (see SC27 N6306) of the 35th SC 27/WG 1 Plenary meeting held in Lucerne (Switzerland), 1st - 5th October 2007, this document is being circulated for **STUDY AND COMMENT**. National Bodies and liaison organizations of SC 27 are requested to send their comments / contributions on the above-mentioned Working Draft by **2008-03-14.**
PLEASE NOTE:	For comments please use THE SC 27 TEMPLATE separately attached to this document.
ACTION:	**COM**
DUE DATE:	**2008-03-14**
DISTRIBUTION:	P-, O- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice Chair T. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	1 + 18

Secretariat ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; E-Mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

ISO/IEC JTC 1/SC 27 N6223

Date: 2007-11-2

ISO/IEC WD 27007

ISO/IEC JTC 1/SC 27/WG 1

Secretariat: DIN

Information technology — Security techniques — Guidelines for information security management systems auditing

Technologies de l'information — Techniques de sécurité

Warning

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

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

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

D:\Eigene Dateien\Project_admin\27007_ISMS_Auditor_Guidelines_27007_May2007\02_01_1stWD_27007_Nov2007\SC27N6222_1stWD_27007_Nov2007\SC27N6222_1stWD_27007_Nov2007.doc STD Version 2.2

Copyright notice

Contents

Page

Foreword

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

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

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

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

ISO/IEC 27007 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Introduction this Standard

ISO 19011 Guidelines for quality and/or environmental management systems auditing is an International Standard which provides guidance on the principles of auditing, managing audit programmes, conducting quality management system audits and environmental management system audits, as well as guidance on the competence of quality and environmental management system auditors.

If organizations want to conduct internal or external audits of Information Security Management Systems (ISMS) in accordance with ISO/IEC 27001:2005, some additional guidance to the standard ISO 19011 are necessary and are provided by this International Standard.

The text in this International Standard follows the structure of ISO 19011, and the additional ISMS-specific guidance on the application of ISO 19011 for ISMS audits are identified by the letters “IS”.

This International Standard provides guidance on the management of audit programmes, the conduct of internal or external audits of ISMSs, as well as on the competence and evaluation of auditors. It is intended to apply to a broad range of potential users, including auditors, organizations implementing ISMSs, organizations needing to conduct audits of ISMSs, and organizations involved in auditor certification or training, in certification/registration of management systems, in accreditation or in standardization in the area of conformity assessment.

[Editor’s Note:** This first WD 27007 uses the currently published version of ISO 19011. As soon as the latest version of the revised ISO 19011 currently under development will be available, the structure of this standard will be adapted to this new version of ISO 19011.**]

Information technology — Security techniques — Guidelines for information security management systems auditing

1 Scope

This International Standard provides guidance on conducting ISMS audits, as well as guidance on the competence of information security management system auditors, in addition to the guidance contained in ISO 19011.

It is applicable to all organizations needing to conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

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 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

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

3 Terms and Definitions

For the purposes of this document, the terms and definitions given in ISO 19011, ISO/IEC 27001 and the following apply.

3.1
XYZ
Text

3.2
XYZ
Text

3.3
XYZ
Text

4 Principles of auditing

The principles of auditing from ISO 19011, Clause 4 apply. In addition, the following ISMS-specific guidance applies.

4.1 IS Principles of auditing

***[Editor's Note:** Any principles related to ISMS auditing that are additional to the general auditing principles are to be added here.*

Is there anything ISMS-specific to add related to issues such as:

Trust: ISMS auditors should not engage in any activities that may endanger the trust in his independence of judgement and integrity in relation to his auditing activities.

*Confidentiality: ISMS auditors should not disclose information gained in audits to unauthorized individuals and entities.**]***

5 Managing an audit programme

5.1 General

The guidelines from ISO 19011, Clause 5.1 apply. In addition, the following ISMS-specific guidance applies.

5.1.1 IS General

[Editor's Note:** Any guidance related to general aspects of managing an ISMS audit programme that is additional to the guidance in ISO 19011 should be added here.**]

5.2 Audit programme objectives and extent

The guidelines from ISO 19011, Clause 5.2 apply. In addition, the following ISMS-specific guidance applies.

5.2.1 IS Audit programme objectives and extent

<u>Combination of Management Systems</u>

If an organization to be audited operates both ISMS and other management system, such as QMS and EMS, and requests auditors to audit them at the same time, combined audits should be included in the audit program.

When conducting a combined audit, auditors will have to be qualified and competent. The audit team, as a whole, should have appropriate technical knowledge and skills that cover all requirements of related standards, and ensure them to be complied with. Remember, never relax ISMS auditing be applied to other management systems.

***[Editor's Note:** Any additional guidance related to the ISMS audit programme objectives and extent that is additional to the guidance in ISO 19011 should be added here.*

Text to be added here should take account of the following contribution:

1. *Specify the extent that the auditor should examine the legal compliance of the organization:*
    a. *the auditor should check that either the organization has a mechanism to regularly check its legal compliance status in information security or the organization could demonstrate that it can effectively detect legal non-compliance incident*

  b. *any legal non-compliance issue identified in the audit process need to be reported to the organization*

2. *Emphasize that the ISMS audit does not intend to replace any legal compliance check or audit that is required by law and regulation to an organization.*

In addition, guidance should be added to address the following important ISMS topics:

- *risk management (including risk assessment and risk treatment)*
- *ISMS measurement (see also ISO/IEC 27004)*
- *ISMS monitoring and review activities*

]

5.3 Audit programme responsibilities, resources and procedures

The guidelines from ISO 19011, Clause 5.3 apply. In addition, the following ISMS-specific guidance applies.

5.3.1 IS Audit programme responsibilities, resources and procedures

[Editor's Note:** Any guidance related to the ISMS audit programme responsibilities, resources and procedures that is additional to the guidance in ISO 19011 should be added here.**]

5.4 Audit programme implementation

The guidelines from ISO 19011, Clause 5.4 apply. In addition, the following ISMS-specific guidance applies.

5.4.1 IS Audit programme implementation

[Editor's Note:** Any guidance related to the ISMS audit programme implementation that is additional to the guidance in ISO 19011 should be added here.**]

5.5 Audit programme records

The guidelines from ISO 19011, Clause 5.5 apply. In addition, the following ISMS-specific guidance applies.

5.5.1 IS Audit programme records

[Editor's Note:** Any guidance related to the ISMS audit programme records that is additional to the guidance in ISO 19011 should be added here.**]

5.6 Audit programme monitoring and review

The guidelines from ISO 19011, Clause 5.6 apply. In addition, the following ISMS-specific guidance applies.

5.6.1 IS Audit programme monitoring and review

[**Editor's Note:** Any guidance related to the ISMS audit programme monitoring and review that is additional to the guidance in ISO 19011 should be added here.**]**

6 Audit activities

6.1 General

The guidelines from ISO 19011, Clause 6.1 apply. In addition, the following ISMS-specific guidance applies.

6.1.1 IS General

[Editor's Note:** Any guidance related to general ISMS audit activities that is additional to the guidance in ISO 19011 should be added here.**]

6.2 Initiating the audit

The guidelines from ISO 19011, Clause 6.2 apply. In addition, the following ISMS-specific guidance applies.

6.2.1 IS Initiating the audit

[Editor's Note:** Any guidance related to initiating the ISMS audit that is additional to the guidance in ISO 19011 should be added here.**]

6.3 Conducting document review

The guidelines from ISO 19011, Clause 6.3 apply. In addition, the following ISMS-specific guidance applies.

6.3.1 IS Conducting document review

Review of ISMS Documents

The mandatory documents required by ISO/IEC 27001:2005 include:

a) Documented statements of the ISMS policy and objectives;

b) The scope of the ISMS;

c) Procedures and controls in support of the ISMS, including

1) Document control procedures;
2) Record control procedures;
3) Internal audit procedures;
4) Procedures for corrective and preventive actions;
5) Management review procedures.

d) A description of the risk assessment methodology;

e) The risk assessment report;

f) The risk treatment plan;

g) Documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls;

h) Records required by ISO/IEC 27005; and

i) The Statement of Applicability.

Auditors should check that all these documents exist and conform to the requirements in ISO/IEC 27001:2005.

[Editor's Note:** Any additional guidance related to conducting document review in an ISMS audit that is additional to the guidance in ISO 19011 should be added here. For example, this could include further guidance on what to look for when reviewing the documents listed above.**]

6.4 Preparing for the on-site audit activities

The guidelines from ISO 19011, Clause 6.4 apply. In addition, the following ISMS-specific guidance applies.

6.4.1 IS Preparing for the on-site audit activities

[Editor's Note:** Any guidance related to preparing for the on-site activities in an ISMS audit that is additional to the guidance in ISO 19011 should be added here.**]

6.5 Conducting on-site audit activities

The guidelines from ISO 19011, Clause 6.5 apply. In addition, the following ISMS-specific guidance applies.

6.5.1 IS Conducting on-site audit activities

Gathering information and evidence

Gathering information and evidence that controls are implemented and effective is an important part of ISMS auditing. One way to do this is system testing, and there are also other means of achieving this objective.

[Editor's Note:** Any additional guidance related to conducting on-site ISMS audit activities that is additional to the guidance in ISO 19011 should be added here, for example more information on how to gather information and evidence.**]

6.6 Preparing, approving and distributing the audit report

The guidelines from ISO 19011, Clause 6.6 apply. In addition, the following ISMS-specific guidance applies.

6.6.1 IS Preparing, approving and distributing the audit report

[Editor's Note:** Any guidance related to preparing, approving and distributing the ISMS audit report that is additional to the guidance in ISO 19011 should be added here.**]

6.7 Completing the audit

The guidelines from ISO 19011, Clause 6.7 apply. In addition, the following ISMS-specific guidance applies.

6.7.1 IS Completing the audit

[Editor's Note:** Any guidance related to completing the ISMS audit that is additional to the guidance in ISO 19011 should be added here.**]

6.8 Conducting audit follow-up

The guidelines from ISO 19011, Clause 6.8 apply. In addition, the following ISMS-specific guidance applies.

6.8.1 IS Conducting audit follow-up

[Editor's Note:** Any guidance related to conducting ISMS audit follow-up that is additional to the guidance in ISO 19011 should be added here.**]

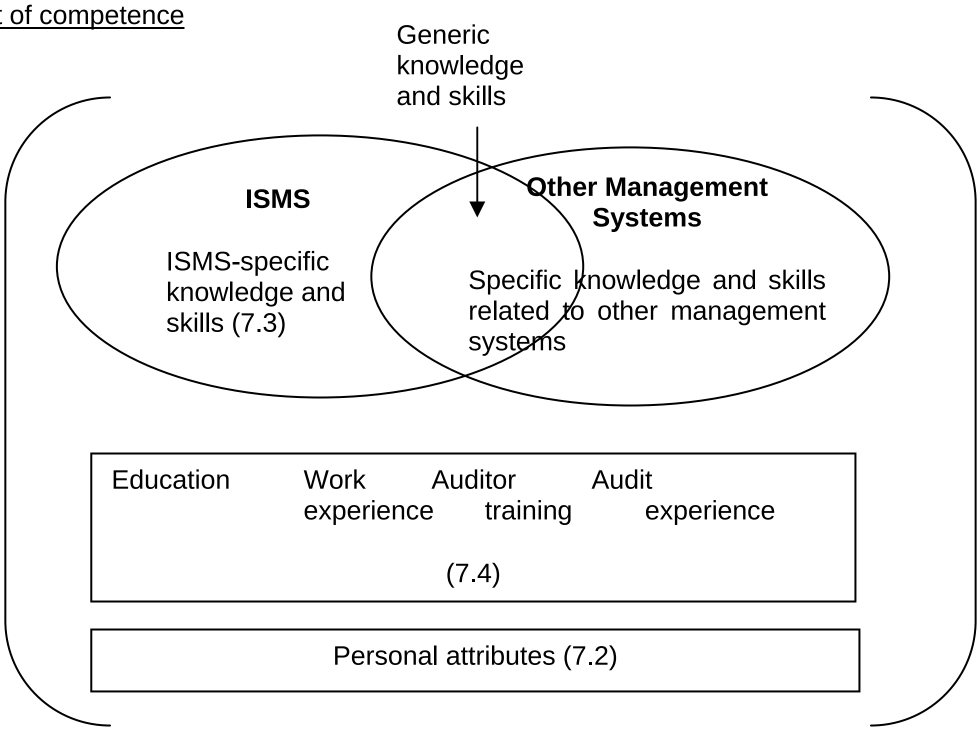
7 Competence and evaluation of auditors

7.1 General

The guidelines from ISO 19011, Clause 7.1 apply. In addition, the following ISMS-specific guidance applies.

7.1.1 IS General

Concept of competence


Generic knowledge and skills
ISMS
ISMS-specific knowledge and skills (7.3)
Other Management Systems
Specific knowledge and skills related to other management systems
Education
Work experience
Auditor training
Audit experience
(7.4)
Personal attributes (7.2)

[Editor's Note:** Any guidance related to general issues regarding competence and evaluation of ISMS auditors that is additional to the guidance in ISO 19011 should be added here.**]

7.2 Personal attributes

The guidelines from ISO 19011, Clause 7.2 apply. In addition, the following ISMS-specific guidance applies.

7.2.1 IS Personal attributes

[Editor's Note:** Any guidance related to personal attributes of ISMS auditors that is additional to the guidance in ISO 19011 should be added here.**]

7.3 Knowledge and skills

The guidelines from ISO 19011, Clause 7.3 apply. In addition, the following ISMS-specific guidance applies.

7.3.1 IS Knowledge and skills

<u>ISMS-specific knowledge and skills</u>

ISMS auditors should have knowledge and skills in the following areas:

a) Information security management methods: to enable the auditor to examine ISMS and generate the appropriate audit findings and recommendations. Knowledge and skills in this area should include:
   1) Information security terminology;
   2) Information security management principles and their application;
   3) Risk management methods and their application.

b) Information security-related techniques, as applicable (for example, physical and logical access control techniques; protection against malicious software; vulnerability management techniques, etc.).

[Editor's Note:** Any guidance related to knowledge and skills of ISMS auditors that is additional to the guidance in ISO 19011 should be added here. Clause 7.3.1 should be consistent with the ISO 27006, section 7, "RESOURCE REQUIREMENTS" and "Annex A.2 Example Areas of Auditor Competence".**]

7.4 Education, work experience, auditor training and audit experience

The guidelines from ISO 19011, Clause 7.4 apply. In addition, the following ISMS-specific guidance applies.

7.4.1 IS Education, work experience, auditor training and audit experience

[Editor's Note:** Any guidance related to education, work experience, ISMS auditor training and ISMS audit experience for ISMS auditors that is additional to the guidance in ISO 19011 should be added here. This should extend the information given in ISO/IEC 27006, Section 7.2, "Personnel involved in the certification activities"**]

7.5 Maintenance and improvement of competence

The guidelines from ISO 19011, Clause 7.5 apply. In addition, the following ISMS-specific guidance applies.

7.5.1 IS Maintenance and improvement of competence

[Editor's Note:** Any guidance related to the maintenance and improvement of competence of ISMS auditors that is additional to the guidance in ISO 19011 should be added here.**]

7.6 Auditor evaluation

The guidelines from ISO 19011, Clause 7.6 apply. In addition, the following ISMS-specific guidance applies.

7.6.1 IS Auditor evaluation

[Editor's Note: *Any guidance related to the evaluation of ISMS auditors that is additional to the guidance in ISO 19011 should be added here.* ***]***

Bibliography

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

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