FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
27001**

ISO/IEC JTC **1**

Secretariat: **DIN**

Voting begins on:
2005-06-30

Voting terminates on:
2005-08-30

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Please see the administrative notes on page iii

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.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 27001:2005(E)

© ISO/IEC 2005

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.

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to 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

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

 © ISO/IEC 2004 – All rights reserved

Contents

Page

Foreword ... iv

0 Introduction ... v
0.1 General ... v
0.2 Process approach ... v
0.3 Compatibility with other management systems ... vi

1 Scope ... 1
1.1 General ... 1
1.2 Application ... 1

2 Normative references ... 1

3 Terms and definitions ... 2

4 Information security management system ... 3
4.1 General requirements ... 3
4.2 Establishing and managing the ISMS ... 4
4.2.1 Establish the ISMS ... 4
4.2.2 Implement and operate the ISMS ... 6
4.2.3 Monitor and review the ISMS ... 6
4.2.4 Maintain and improve the ISMS ... 7
4.3 Documentation requirements ... 7
4.3.1 General ... 7
4.3.2 Control of documents ... 8
4.3.3 Control of records ... 8

5 Management responsibility ... 9
5.1 Management commitment ... 9
5.2 Resource management ... 9
5.2.1 Provision of resources ... 9
5.2.2 Training, awareness and competence ... 9

6 Internal ISMS audits ... 10

7 Management review of the ISMS ... 10
7.1 General ... 10
7.2 Review input ... 10
7.3 Review output ... 11

8 ISMS improvement ... 11
8.1 Continual improvement ... 11
8.2 Corrective action ... 11
8.3 Preventive action ... 12

Annex A (normative) **Control objectives and controls** ... 13

Annex B (informative) **OECD principles and this International Standard** ... 30

Annex C (informative) **Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard** ... 31

Bibliography ... 34

© ISO/IEC 2005 – All rights reserved

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 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2005 – All rights reserved

0 Introduction

0.1 General

This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.

This International Standard can be used in order to assess conformance by interested internal and external parties.

0.2 Process approach

This International Standard promotes the adoption of a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the following process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

a) understanding an organization's information security requirements and the need to establish policy and objectives for information security;

b) implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;

c) monitoring and reviewing the performance and effectiveness of the ISMS; and

d) continual improvement based on objective measurement.

This International Standard adopts the "Plan-Do-Check-Act" (PDCA) process model, which is applied to structure all ISMS processes. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations. Figure 1 also illustrates the links in the processes presented in Clauses 4, 5, 6, 7 and 8.

The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines (2002)[1)] governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

1) OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

© ISO/IEC 2005 – All rights reserved

EXAMPLE 1

A requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization.

EXAMPLE 2

An expectation might be that if a serious incident occurs — perhaps hacking of an organization's eBusiness web site — there should be people with sufficient training in appropriate procedures to minimize the impact.

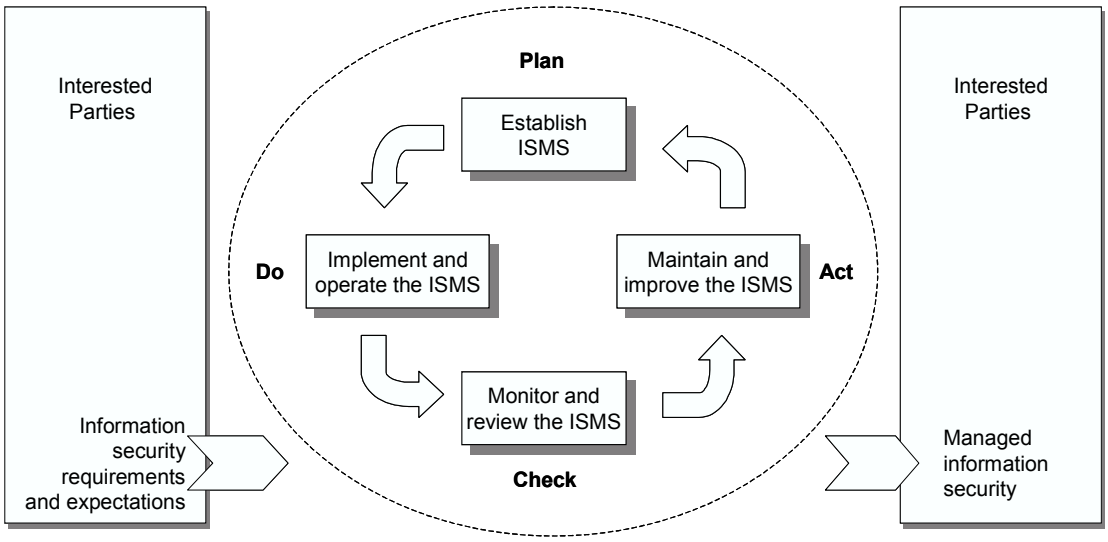

Figure 1 — PDCA model applied to ISMS processes

Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

0.3 Compatibility with other management systems

This International Standard is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can thus satisfy the requirements of all these standards. Table C.1 illustrates the relationship between the clauses of this International Standard, ISO 9001:2000 and ISO 14001:2004.

This International Standard is designed to enable an organization to align or integrate its ISMS with related management system requirements.

© ISO/IEC 2005 – All rights reserved

Information technology — Security techniques — Information security management systems — Requirements

IMPORTANT — This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application. Compliance with an International Standard does not in itself confer immunity from legal obligations.

1 Scope

1.1 General

This International Standard covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

NOTE 1: References to 'business' in this International Standard should be interpreted broadly to mean those activities that are core to the purposes for the organization's existence.

NOTE 2: ISO/IEC 17799 provides implementation guidance that can be used when designing controls.

1.2 Application

The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size and nature. Excluding any of the requirements specified in Clauses 4, 5, 6, 7, and 8 is not acceptable when an organization claims conformity to this International Standard.

Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons. Where any controls are excluded, claims of conformity to this International Standard are not acceptable unless such exclusions do not affect the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable regulatory requirements.

NOTE: If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within this existing management system.

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 17799:2005, *Information technology — Security techniques — Code of practice for information security management.*

© ISO/IEC 2005 – All rights reserved

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
asset
anything that has value to the organization

[ISO/IEC 13335-1:2004]

3.2
availability
the property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 13335-1:2004]

3.3
confidentiality
the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-1:2004]

3.4
information security
preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

[ISO/IEC 17799:2005]

3.5
information security event
an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

[ISO/IEC TR 18044:2004]

3.6
information security incident
a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

[ISO/IEC TR 18044:2004]

3.7
information security management system
ISMS
that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.8
integrity
the property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004]

3.9
residual risk
the risk remaining after risk treatment

[ISO/IEC Guide 73:2002]

© ISO/IEC 2005 – All rights reserved

3.10
risk acceptance
decision to accept a risk

[ISO/IEC Guide 73:2002]

3.11
risk analysis
systematic use of information to identify sources and to estimate the risk

[ISO/IEC Guide 73:2002]

3.12
risk assessment
overall process of risk analysis and risk evaluation

[ISO/IEC Guide 73:2002]

3.13
risk evaluation
process of comparing the estimated risk against given risk criteria to determine the significance of the risk

[ISO/IEC Guide 73:2002]

3.14
risk management
coordinated activities to direct and control an organization with regard to risk

[ISO/IEC Guide 73:2002]

3.15
risk treatment
process of selection and implementation of measures to modify risk

[ISO/IEC Guide 73:2002]

NOTE: In this International Standard the term ‘control’ is used as a synonym for ‘measure’.

3.16
statement of applicability
documented statement describing the control objectives and controls that are relevant and applicable to the organization’s ISMS.

NOTE: Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization’s business requirements for information security.

4 Information security management system

4.1 General requirements

The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organization’s overall business activities and the risks they face. For the purposes of this International Standard the process used is based on the PDCA model shown in Figure 1.

© ISO/IEC 2005 – All rights reserved

4.2 Establishing and managing the ISMS

4.2.1 Establish the ISMS

The organization shall do the following.

a) Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets, technology, and including details of and justification for any exclusions from the scope (see 1.2).

b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology that:

   1) includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security;

   2) takes into account business and legal or regulatory requirements, and contractual security obligations;

   3) aligns with the organization's strategic risk management context in which the establishment and maintenance of the ISMS will take place;

   4) establishes criteria against which risk will be evaluated (see 4.2.1c));

   5) has been approved by management.

   NOTE: For the purposes of this International Standard, the ISMS policy is considered as a superset of the information security policy. These policies can be described in one document.

c) Define the risk assessment approach of the organization.

   1) Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.

   2) Develop criteria for accepting risks and identify the acceptable levels of risk. (see 5.1f)).

   The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results.

   NOTE: There are different methodologies for risk assessment. Examples of risk assessment methodologies are discussed in ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Techniques for the management of IT Security*.

d) Identify the risks.

   1) Identify the assets within the scope of the ISMS, and the owners[2)] of these assets.

   2) Identify the threats to those assets.

   3) Identify the vulnerabilities that might be exploited by the threats.

   4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

---

2) The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset.

© ISO/IEC 2005 – All rights reserved

e) Analyse and evaluate the risks.

1) Assess the business impact upon the organization that might result from a security failure, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets.

2) Assess the realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.

3) Estimate the levels of risks.

4) Determine whether the risk is acceptable or requires treatment using the risk acceptance criteria established in 4.2.1c)2).

f) Identify and evaluate options for the treatment of risks.

Possible actions include:

1) applying appropriate controls;

2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policies and the criteria for risk acceptance (see 4.2.1c)2));

3) avoiding risks; and

4) transferring the associated business risks to other parties, e.g. insurers, suppliers.

g) Select control objectives and controls for the treatment of risks.

Controls objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection shall take account of the criteria for accepting risks (see 4.2.1c)) as well as legal, regulatory and contractual requirements.

The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover these requirements.

The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

NOTE: Annex A contains a comprehensive list of control objectives and controls that have been found to be commonly relevant in organizations. Users of this International Standard are directed to Annex A as a starting point for control selection to ensure that no important control options are overlooked.

h) Obtain management approval of the proposed residual risks.

i) Obtain management authorization to implement and operate the ISMS.

j) Prepare a Statement of Applicability.

A Statement of Applicability shall be prepared that includes the following:

1) the control objectives and controls, selected in 4.2.1g) and the reasons for their selection;

2) the control objectives and controls currently implemented (see 4.2.1e)2)); and

3) the exclusion of any control objectives and controls in Annex A and the justification for their exclusion.

NOTE: The Statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted.

© ISO/IEC 2005 – All rights reserved

4.2.2 Implement and operate the ISMS

The organization shall do the following.

a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks (see 5).

b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.

c) Implement controls selected in 4.2.1g) to meet the control objectives.

d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3c)).

NOTE: Measuring the effectiveness of controls allow managers and staff to determine how well controls achieve planned control objectives.

e) Implement training and awareness programmes (see 5.2.2).

f) Manage operations of the ISMS.

g) Manage resources for the ISMS (see 5.2).

h) Implement procedures and other controls capable of enabling prompt detection of and response to security incidents (see 4.2.3).

4.2.3 Monitor and review the ISMS

The organization shall do the following.

a) Execute monitoring and review procedures and other controls to:

1) promptly detect errors in the results of processing;

2) promptly identify attempted and successful security breaches and incidents;

3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;

4) help detect security events and thereby prevent security incidents by the use of indicators; and

5) determine whether the actions taken to resolve a breach of security were effective.

b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, effectiveness measurements, suggestions and feedback from all interested parties.

c) Measure the effectiveness of controls to verify that security requirements have been met.

d) Review risk assessments at planned intervals and review the level of residual risk and identified acceptable risk, taking into account changes to:

1) the organization;

2) technology;

3) business objectives and processes;

 © ISO/IEC 2005 – All rights reserved

4) identified threats;

5) effectiveness of the implemented controls; and

6) external events, such as changes to the legal or regulatory environment, changed contractual obligations, and changes in social climate.

e) Conduct internal ISMS audits at planned intervals (see 6).

NOTE: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself for internal purposes.

f) Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified (see 7.1).

g) Update security plans to take into account the findings of monitoring and reviewing activities.

h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3).

4.2.4 Maintain and improve the ISMS

The organization shall regularly do the following.

a) Implement the identified improvements in the ISMS.

b) Take appropriate corrective and preventive actions in accordance with 8.2 and 8.3. Apply the lessons learnt from the security experiences of other organizations and those of the organization itself.

c) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

d) Ensure that the improvements achieve their intended objectives.

4.3 Documentation requirements

4.3.1 General

Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and the recorded results are reproducible.

It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.

The ISMS documentation shall include:

a) documented statements of the ISMS policy (see 4.2.1b)) and objectives;

b) the scope of the ISMS (see 4.2.1a));

c) procedures and controls in support of the ISMS;

d) a description of the risk assessment methodology (see 4.2.1c));

e) the risk assessment report (see 4.2.1c) to 4.2.1g));

f) the risk treatment plan (see 4.2.2b));

© ISO/IEC 2005 – All rights reserved

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 (see 4.2.3c));

h) records required by this International Standard (see 4.3.3); and

i) the Statement of Applicability.

NOTE 1: Where the term “documented procedure” appears within this International Standard, this means that the procedure is established, documented, implemented and maintained.

NOTE 2: The extent of the ISMS documentation can differ from one organization to another owing to:

- the size of the organization and the type of its activities; and
- the scope and complexity of the security requirements and the system being managed.

NOTE 3: Documents and records may be in any form or type of medium.

4.3.2 Control of documents

Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:

a) approve documents for adequacy prior to issue;

b) review and update documents as necessary and re-approve documents;

c) ensure that changes and the current revision status of documents are identified;

d) ensure that relevant versions of applicable documents are available at points of use;

e) ensure that documents remain legible and readily identifiable;

f) ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification;

g) ensure that documents of external origin are identified;

h) ensure that the distribution of documents is controlled;

i) prevent the unintended use of obsolete documents; and

j) apply suitable identification to them if they are retained for any purpose.

4.3.3 Control of records

Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be protected and controlled. The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. Records shall remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.

Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security incidents related to the ISMS.

EXAMPLE

Examples of records are a visitors’ book, audit reports and completed access authorization forms.

© ISO/IEC 2005 – All rights reserved

5 Management responsibility

5.1 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a) establishing an ISMS policy;

b) ensuring that ISMS objectives and plans are established;

c) establishing roles and responsibilities for information security;

d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;

e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1);

f) deciding the criteria for accepting risks and for acceptable risk levels;

g) ensuring that internal ISMS audits are conducted (see 6); and

h) conducting management reviews of the ISMS (see 7).

5.2 Resource management

5.2.1 Provision of resources

The organization shall determine and provide the resources needed to:

a) establish, implement, operate, monitor, review, maintain and improve an ISMS;

b) ensure that information security procedures support the business requirements;

c) identify and address legal and regulatory requirements and contractual security obligations;

d) maintain adequate security by correct application of all implemented controls;

e) carry out reviews when necessary, and to react appropriately to the results of these reviews; and

f) where required, improve the effectiveness of the ISMS.

5.2.2 Training, awareness and competence

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

a) determining the necessary competencies for personnel performing work effecting the ISMS;

b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;

c) evaluating the effectiveness of the actions taken; and

d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3).

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

© ISO/IEC 2005 – All rights reserved

6 Internal ISMS audits

The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:

a) conform to the requirements of this International Standard and relevant legislation or regulations;

b) conform to the identified information security requirements;

c) are effectively implemented and maintained; and

d) perform as expected.

An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results (see 8).

NOTE: ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*, may provide helpful guidance for carrying out the internal ISMS audits.

7 Management review of the ISMS

7.1 General

Management shall review the organization's ISMS at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. The results of the reviews shall be clearly documented and records shall be maintained (see 4.3.3).

7.2 Review input

The input to a management review shall include:

a) results of ISMS audits and reviews;

b) feedback from interested parties;

c) techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness;

d) status of preventive and corrective actions;

e) vulnerabilities or threats not adequately addressed in the previous risk assessment;

f) results from effectiveness measurements;

g) follow-up actions from previous management reviews;

h) any changes that could affect the ISMS; and

i) recommendations for improvement.

© ISO/IEC 2005 – All rights reserved

7.3 Review output

The output from the management review shall include any decisions and actions related to the following.

a) Improvement of the effectiveness of the ISMS.

b) Update of the risk assessment and risk treatment plan.

c) Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:

   1) business requirements;

   2) security requirements;

   3) business processes effecting the existing business requirements;

   4) regulatory or legal requirements;

   5) contractual obligations; and

   6) levels of risk and/or risk acceptance criteria.

d) Resource needs.

e) Improvement to how the effectiveness of controls is being measured.

8 ISMS improvement

8.1 Continual improvement

The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review (see 7).

8.2 Corrective action

The organization shall take action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence. The documented procedure for corrective action shall define requirements for:

a) identifying nonconformities;

b) determining the causes of nonconformities;

c) evaluating the need for actions to ensure that nonconformities do not recur;

d) determining and implementing the corrective action needed;

e) recording results of action taken (see 4.3.3); and

f) reviewing of corrective action taken.

© ISO/IEC 2005 – All rights reserved

8.3 Preventive action

The organization shall determine action to eliminate the cause of potential nonconformities with the ISMS requirements in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:

a) identifying potential nonconformities and their causes;

b) evaluating the need for action to prevent occurrence of nonconformities;

c) determining and implementing preventive action needed;

d) recording results of action taken (see 4.3.3); and

e) reviewing of preventive action taken.

The organization shall identify changed risks and identify preventive action requirements focusing attention on significantly changed risks.

The priority of preventive actions shall be determined based on the results of the risk assessment.

NOTE: Action to prevent nonconformities is often more cost-effective than corrective action.

© ISO/IEC 2005 – All rights reserved

Annex A
(normative)

Control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 17799:2005 Clauses 5 to 15. The lists in these tables are not exhaustive and an organization may consider that additional control objectives and controls are necessary. Control objectives and controls from these tables shall be selected as part of the ISMS process specified in 4.2.1.

ISO/IEC 17799:2005 Clauses 5 to 15 provide implementation advice and guidance on best practice in support of the controls specified in A.5 to A.15.

Table A.1 – Control objectives and controls

A.5 Security policy		
A.5.1 Information security policy *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Information security policy document	*Control* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
A.5.1.2	Review of the information security policy	*Control* The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
A.6 Organization of information security		
A.6.1 Internal organization *Objective:* To manage information security within the organization.		
A.6.1.1	Management commitment to information security	*Control* Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
A.6.1.2	Information security co-ordination	*Control* Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
A.6.1.3	Allocation of information security responsibilities	*Control* All information security responsibilities shall be clearly defined.

© ISO/IEC 2005 – All rights reserved

A.6.1.4	Authorization process for information processing facilities	*Control* A management authorization process for new information processing facilities shall be defined and implemented.
A.6.1.5	Confidentiality agreements	*Control* Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
A.6.1.6	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.
A.6.1.7	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.8	Independent review of information security	*Control* The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.
A.6.2 External parties *Objective:* To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.		
A.6.2.1	Identification of risks related to external parties	*Control* The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
A.6.2.2	Addressing security when dealing with customers	*Control* All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
A.6.2.3	Addressing security in third party agreements	*Control* Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

© ISO/IEC 2005 – All rights reserved

A.7 Asset management		
A.7.1 Responsibility for assets *Objective:* To achieve and maintain appropriate protection of organizational assets.		
A.7.1.1	Inventory of assets	*Control* All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
A.7.1.2	Ownership of assets	*Control* All information and assets associated with information processing facilities shall be 'owned' [3] by a designated part of the organization.
A.7.1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.
A.7.2 Information classification *Objective:* To ensure that information receives an appropriate level of protection.		
A.7.2.1	Classification guidelines	*Control* Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
A.7.2.2	Information labelling and handling	*Control* An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
A.8 Human resources security		
A.8.1 Prior to employment [4] *Objective:* To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.		
A.8.1.1	Roles and responsibilities	*Control* Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

[3] Explanation: The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has property rights to the asset.

[4] Explanation: The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.

© ISO/IEC 2005 – All rights reserved

A.8.1.2	Screening	*Control* Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
A.8.1.3	Terms and conditions of employment	*Control* As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.
A.8.2 During employment *Objective:* To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.		
A.8.2.1	Management responsibilities	*Control* Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.
A.8.2.2	Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
A.8.2.3	Disciplinary process	*Control* There shall be a formal disciplinary process for employees who have committed a security breach.
A.8.3 Termination or change of employment *Objective:* To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.		
A.8.3.1	Termination responsibilities	*Control* Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.
A.8.3.2	Return of assets	*Control* All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
A.8.3.3	Removal of access rights	*Control* The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

© ISO/IEC 2005 – All rights reserved

A.9 Physical and environmental security		
A.9.1 Secure areas *Objective:* To prevent unauthorized physical access, damage and interference to the organization's premises and information.		
A.9.1.1	Physical security perimeter	*Control* Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
A.9.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.9.1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms, and facilities shall be designed and applied.
A.9.1.4	Protecting against external and environmental threats	*Control* Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.
A.9.1.5	Working in secure areas	*Control* Physical protection and guidelines for working in secure areas shall be designed and applied.
A.9.1.6	Public access, delivery and loading areas	*Control* Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
A.9.2 Equipment security *Objective:* To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.		
A.9.2.1	Equipment siting and protection	*Control* Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.9.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.9.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

© ISO/IEC 2005 – All rights reserved

A.9.2.4	Equipment maintenance	*Control* Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.9.2.5	Security of equipment off-premises	*Control* Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
A.9.2.6	Secure disposal or re-use of equipment	*Control* All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
A.9.2.7	Removal of property	*Control* Equipment, information or software shall not be taken off-site without prior authorization.
A.10 Communications and operations management		
A.10.1 Operational procedures and responsibilities *Objective:* To ensure the correct and secure operation of information processing facilities.		
A.10.1.1	Documented operating procedures	*Control* Operating procedures shall be documented, maintained, and made available to all users who need them.
A.10.1.2	Change management	*Control* Changes to information processing facilities and systems shall be controlled.
A.10.1.3	Segregation of duties	*Control* Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.10.1.4	Separation of development, test and operational facilities	*Control* Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.
A.10.2 Third party service delivery management *Objective:* To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.		
A.10.2.1	Service delivery	*Control* It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

© ISO/IEC 2005 – All rights reserved

A.10.2.2	Monitoring and review of third party services	*Control* The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
A.10.2.3	Managing changes to third party services	*Control* Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
A.10.3 System planning and acceptance *Objective:* To minimize the risk of systems failures.		
A.10.3.1	Capacity management	*Control* The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
A.10.3.2	System acceptance	*Control* Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
A.10.4 Protection against malicious and mobile code *Objective:* To protect the integrity of software and information.		
A.10.4.1	Controls against malicious code	*Control* Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
A.10.4.2	Controls against mobile code	*Control* Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.
A.10.5 Back-up *Objective:* To maintain the integrity and availability of information and information processing facilities.		
A.10.5.1	Information back-up	*Control* Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

© ISO/IEC 2005 – All rights reserved

A.10.6 Network security management *Objective:* To ensure the protection of information in networks and the protection of the supporting infrastructure.		
A.10.6.1	Network controls	*Control* Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
A.10.6.2	Security of network services	*Control* Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
A.10.7 Media handling *Objective:* To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.		
A.10.7.1	Management of removable media	*Control* There shall be procedures in place for the management of removable media.
A.10.7.2	Disposal of media	*Control* Media shall be disposed of securely and safely when no longer required, using formal procedures.
A.10.7.3	Information handling procedures	*Control* Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
A.10.7.4	Security of system documentation	*Control* System documentation shall be protected against unauthorized access.
A.10.8 Exchange of information *Objective:* To maintain the security of information and software exchanged within an organization and with any external entity.		
A.10.8.1	Information exchange policies and procedures	*Control* Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.
A.10.8.2	Exchange agreements	*Control* Agreements shall be established for the exchange of information and software between the organization and external parties.
A.10.8.3	Physical media in transit	*Control* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

© ISO/IEC 2005 – All rights reserved

A.10.8.4	Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.
A.10.8.5	Business information systems	*Control* Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.
A.10.9 Electronic commerce services *Objective:* To ensure the security of electronic commerce services, and their secure use.		
A.10.9.1	Electronic commerce	*Control* Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
A.10.9.2	On-line transactions	*Control* Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.10.9.3	Publicly available information	*Control* The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
A.10.10 Monitoring *Objective:* To detect unauthorized information processing activities.		
A.10.10.1	Audit logging	*Control* Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
A.10.10.2	Monitoring system use	*Control* Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
A.10.10.3	Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access.
A.10.10.4	Administrator and operator logs	*Control* System administrator and system operator activities shall be logged.
A.10.10.5	Fault logging	*Control* Faults shall be logged, analyzed, and appropriate action taken.

© ISO/IEC 2005 – All rights reserved

A.10.10.6	Clock synchronization	*Control* The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.
A.11 Access control		
A.11.1 Business requirement for access control *Objective:* To control access to information.		
A.11.1.1	Access control policy	*Control* An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
A.11.2 User access management *Objective:* To ensure authorized user access and to prevent unauthorized access to information systems.		
A.11.2.1	User registration	*Control* There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
A.11.2.2	Privilege management	*Control* The allocation and use of privileges shall be restricted and controlled.
A.11.2.3	User password management	*Control* The allocation of passwords shall be controlled through a formal management process.
A.11.2.4	Review of user access rights	*Control* Management shall review users' access rights at regular intervals using a formal process.
A.11.3 User responsibilities *Objective:* To prevent unauthorized user access, and compromise or theft of information and information processing facilities.		
A.11.3.1	Password use	*Control* Users shall be required to follow good security practices in the selection and use of passwords.
A.11.3.2	Unattended user equipment	*Control* Users shall ensure that unattended equipment has appropriate protection.
A.11.3.3	Clear desk and clear screen policy	*Control* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

© ISO/IEC 2005 – All rights reserved

A.11.4 Network access control *Objective:* To prevent unauthorized access to networked services.		
A.11.4.1	Policy on use of network services	*Control* Users shall only be provided with access to the services that they have been specifically authorized to use.
A.11.4.2	User authentication for external connections	*Control* Appropriate authentication methods shall be used to control access by remote users.
A.11.4.3	Equipment identification in networks	*Control* Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.
A.11.4.4	Remote diagnostic and configuration port protection	*Control* Physical and logical access to diagnostic and configuration ports shall be controlled.
A.11.4.5	Segregation in networks	*Control* Groups of information services, users, and information systems shall be segregated on networks.
A.11.4.6	Network connection control	*Control* For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).
A.11.4.7	Network routing control	*Control* Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
A.11.5 Operating system access control *Objective:* To prevent unauthorized access to operating systems.		
A.11.5.1	Secure log-on procedures	*Control* Access to operating systems shall be controlled by a secure log-on procedure.
A.11.5.2	User identification and authentication	*Control* All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
A.11.5.3	Password management system	*Control* Systems for managing passwords shall be interactive and shall ensure quality passwords.

© ISO/IEC 2005 – All rights reserved

A.11.5.4	Use of system utilities	*Control* The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.11.5.5	Session time-out	*Control* Inactive sessions shall shut down after a defined period of inactivity.
A.11.5.6	Limitation of connection time	*Control* Restrictions on connection times shall be used to provide additional security for high-risk applications.
A.11.6 Application and information access control *Objective:* To prevent unauthorized access to information held in application systems.		
A.11.6.1	Information access restriction	*Control* Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.
A.11.6.2	Sensitive system isolation	*Control* Sensitive systems shall have a dedicated (isolated) computing environment.
A.11.7 Mobile computing and teleworking *Objective:* To ensure information security when using mobile computing and teleworking facilities.		
A.11.7.1	Mobile computing and communications	*Control* A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.
A.11.7.2	Teleworking	*Control* A policy, operational plans and procedures shall be developed and implemented for teleworking activities.
A.12 Information systems acquisition, development and maintenance		
A.12.1 Security requirements of information systems *Objective:* To ensure that security is an integral part of information systems.		
A.12.1.1	Security requirements analysis and specification	*Control* Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

© ISO/IEC 2005 – All rights reserved

A.12.2 Correct processing in applications *Objective:* To prevent errors, loss, unauthorized modification or misuse of information in applications.		
A.12.2.1	Input data validation	*Control* Data input to applications shall be validated to ensure that this data is correct and appropriate.
A.12.2.2	Control of internal processing	*Control* Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
A.12.2.3	Message integrity	*Control* Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
A.12.2.4	Output data validation	*Control* Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
A.12.3 Cryptographic controls *Objective:* To protect the confidentiality, authenticity or integrity of information by cryptographic means.		
A.12.3.1	Policy on the use of cryptographic controls	*Control* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.12.3.2	Key management	*Control* Key management shall be in place to support the organization's use of cryptographic techniques.
A.12.4 Security of system files *Objective:* To ensure the security of system files.		
A.12.4.1	Control of operational software	*Control* There shall be procedures in place to control the installation of software on operational systems.
A.12.4.2	Protection of system test data	*Control* Test data shall be selected carefully, and protected and controlled.
A.12.4.3	Access control to program source code	*Control* Access to program source code shall be restricted.

© ISO/IEC 2005 – All rights reserved

A.12.5 Security in development and support processes *Objective:* To maintain the security of application system software and information.		
A.12.5.1	Change control procedures	*Control* The implementation of changes shall be controlled by the use of formal change control procedures.
A.12.5.2	Technical review of applications after operating system changes	*Control* When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.12.5.3	Restrictions on changes to software packages	*Control* Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.
A.12.5.4	Information leakage	*Control* Opportunities for information leakage shall be prevented.
A.12.5.5	Outsourced software development	*Control* Outsourced software development shall be supervised and monitored by the organization.
A.12.6 Technical Vulnerability Management *Objective:* To reduce risks resulting from exploitation of published technical vulnerabilities.		
A.12.6.1	Control of technical vulnerabilities	*Control* Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
A.13 Information security incident management		
A.13.1 Reporting information security events and weaknesses *Objective:* To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.		
A.13.1.1	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.
A.13.1.2	Reporting security weaknesses	*Control* All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

© ISO/IEC 2005 – All rights reserved

A.13.2 Management of information security incidents and improvements *Objective:* To ensure a consistent and effective approach is applied to the management of information security incidents.		
A.13.2.1	Responsibilities and procedures	*Control* Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
A.13.2.2	Learning from information security incidents	*Control* There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
A.13.2.3	Collection of evidence	*Control* Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
A.14 Business continuity management		
A.14.1 Information security aspects of business continuity management *Objective:* To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.		
A.14.1.1	Including information security in the business continuity management process	*Control* A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
A.14.1.2	Business continuity and risk assessment	*Control* Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
A.14.1.3	Developing and implementing continuity plans including information security	*Control* Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
A.14.1.4	Business continuity planning framework	*Control* A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
A.14.1.5	Testing, maintaining and re-assessing business continuity plans	*Control* Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

© ISO/IEC 2005 – All rights reserved

A.15 Compliance		
A.15.1 Compliance with legal requirements *Objective:* To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.		
A.15.1.1	Identification of applicable legislation	*Control* All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
A.15.1.2	Intellectual property rights (IPR)	*Control* Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
A.15.1.3	Protection of organizational records	*Control* Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
A.15.1.4	Data protection and privacy of personal information	*Control* Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
A.15.1.5	Prevention of misuse of information processing facilities	*Control* Users shall be deterred from using information processing facilities for unauthorized purposes.
A.15.1.6	Regulation of cryptographic controls	*Control* Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
A.15.2 Compliance with security policies and standards, and technical compliance *Objective:* To ensure compliance of systems with organizational security policies and standards.		
A.15.2.1	Compliance with security policies and standards	*Control* Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
A.15.2.2	Technical compliance checking	*Control* Information systems shall be regularly checked for compliance with security implementation standards.

© ISO/IEC 2005 – All rights reserved

A.15.3 Information systems audit considerations *Objective:* To maximize the effectiveness of and to minimize interference to/from the information systems audit process.		
A.15.3.1	Information systems audit controls	*Control* Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
A.15.3.2	Protection of information systems audit tools	*Control* Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

© ISO/IEC 2005 – All rights reserved

Annex B
(informative)

OECD principles and this International Standard

The principles given in the OECD Guidelines for the Security of Information Systems and Networks [1] apply to all policy and operational levels that govern the security of information systems and networks. This International Standard provides an information security management system framework for implementing some of the OECD principles using the PDCA model and the processes described in Clauses 4, 5, 6 and 8, as indicated in Table B.1.

Table B.1 — OECD principles and the PDCA model

OECD principle	Corresponding ISMS process and PDCA phase
Awareness Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.	This activity is part of the **Do** phase (see 4.2.2 and **5.2.2**).
Responsibility All participants are responsible for the security of information systems and networks.	This activity is part of the **Do** phase (see 4.2.2 and **5.1**).
Response Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.	This is in part a monitoring activity **Check** phase (see 4.2.3 and 6 to 7.3 and a responding activity **Act** phase (see 4.2.4 and 8.1 to 8.3). This can also be covered by some aspects of the **Plan** and **Check** phases.
Risk assessment Participants should conduct risk assessments.	This activity is part of the **Plan** phase (see 4.2.1) and risk reassessment is part of the **Check** phase (see 4.2.3 and 6 to 7.3).
Security design and implementation Participants should incorporate security as an essential element of information systems and networks.	Once a risk assessment has been completed, controls are selected for the treatment of risks as part of the **Plan** phase (see 4.2.1). The **Do** phase (see 4.2.2 and 5.2) then covers the implementation and operational use of these controls.
Security management Participants should adopt a comprehensive approach to security management.	The management of risk is a process which includes the prevention, detection and response to incidents, ongoing maintenance, review and audit. All of these aspects are encompassed in the **Plan**, **Do**, **Check** and **Act** phases.
Reassessment Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.	Reassessment of information security is a part of the **Check** phase (see 4.2.3 and 6 to 7.3) where regular reviews should be undertaken to check the effectiveness of the information security management system, and improving the security is part of the **Act** phase (see 4.2.4 and 8.1 to 8.3).

© ISO/IEC 2005 – All rights reserved

Annex C
(informative)

Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard

Table C.1 shows the correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard.

Table C.1 — Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard

This International Standard	ISO 9001:2000	ISO 14001:2004
Introduction	**0 Introduction**	**Introduction**
General	0.1 General	
Process approach	0.2 Process approach	
	0.3 Relationship with ISO 9004	
Compatibility with other management systems	0.4 Compatibility with other management systems	
1 Scope	**1 Scope**	**1 Scope**
1.1 General	1.1 General	
1.2 Application	1.2 Application	
2 Normative references	**2 Normative reference**	**2 Normative reference**
3 Terms and definitions	**3 Terms and definitions**	**3 Terms and definitions**
4 Information security management system	**4 Quality management system**	**4 EMS requirements**
4.1 General requirements	4.1 General requirements	4.1 General requirements
4.2 Establishing and managing the ISMS		
4.2.1 Establish the ISMS		
4.2.2 Implement and operate the ISMS		4.4 Implementation and operation
4.2.3 Monitor and review the ISMS	8.2.3 Monitoring and measurement of processes	4.5.1 Monitoring and measurement
	8.2.4 Monitoring and measurement of product	

© ISO/IEC 2005 – All rights reserved

This International Standard	ISO 9001:2000	ISO 14001:2004
4.2.4 Maintain and improve the ISMS		
4.3 Documentation requirements 4.3.1 General 4.3.2 Control of documents 4.3.3 Control of records	4.2 Documentation requirements 4.2.1 General 4.2.2 Quality manual 4.2.3 Control of documents 4.2.4 Control of records	 4.4.5 Documentation control 4.5.4 Control of records
5 Management responsibility 5.1 Management commitment	**5 Management responsibility** 5.1 Management commitment 5.2 Customer focus 5.3 Quality policy 5.4 Planning 5.5 Responsibility, authority and communication	 4.2 Environmental policy 4.3 Planning
5.2 Resource management 5.2.1 Provision of resources 5.2.2 Training, awareness and competence	**6 Resource management** 6.1 Provision of resources 6.2 Human resources 6.2.2 Competence, awareness and training 6.3 Infrastructure 6.4 Work environment	 4.4.2 Competence, training, and awareness
6 Internal ISMS audits	8.2.2 Internal Audit	4.5.5 Internal audit
7 Management review of the ISMS 7.1 General 7.2 Review input 7.3 Review output	**5.6 Management review** 5.6.1 General 5.6.2 Review input 5.6.3 Review output	**4.6 Management review**
8 ISMS improvement 8.1 Continual improvement	**8.5 Improvement** 8.5.2 Continual improvement	

© ISO/IEC 2005 – All rights reserved

This International Standard	ISO 9001:2000	ISO 14001:2004
8.2 Corrective action	8.5.3 Corrective actions	4.5.3 Non-conformity, corrective action and preventive action
8.3 Preventive action	8.5.3 Preventive actions	
Annex A Control objectives and controls **Annex B OECD principles and this International Standard** **Annex C Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard**	**Annex A Correspondence between ISO 9001:2000 and ISO 14001:1996**	**Annex A Guidance on the use of this International Standard** **Annex B Correspondence between ISO 14001:2004 and ISO 9001:2000**

© ISO/IEC 2005 – All rights reserved

Bibliography

Standards publications

[1] ISO 9001:2000*, Quality management systems — Requirements*

[2] ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[3] ISO/IEC TR 13335-3:1998, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security*

[4] ISO/IEC TR 13335-4:2000, *Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards*

[5] ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*

[6] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management*

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

[8] ISO/IEC Guide 62:1996, *General requirements for bodies operating assessment and certification/registration of quality systems*

[9] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

Other publications

[1] OECD, *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org*

[2] NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

[3] Deming W.E., Out *of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986*

© ISO/IEC 2005 – All rights reserved

ICS 35.040

Price based on 34 pages

© ISO/IEC 2004 – All rights reserved