



## DRAFT INTERNATIONAL STANDARD ISO/DIS 28000

ISO/TC 8

Secretariat: JISC

Voting begins on:  
**2006-09-01**

Voting terminates on:  
**2007-02-01**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

# Specification for security management systems for the supply chain

*Spécifications pour les systèmes de management de la sûreté pour la chaîne d'approvisionnement*

[Revision of the first edition (ISO/PAS 28000:2005)]

ICS 47.020.99

**In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.**

**Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.**

**To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.**

**Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.**

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

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.

**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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

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

Violators may be prosecuted.

<b>Contents</b>	<b>Page</b>
<b>Foreword .....</b>	<b>iv</b>
<b>Introduction</b>	
<b>1 Scope</b>	
<b>2 Normative references</b>	
<b>3 Terms and definitions</b>	
<b>4 Security management system elements</b>	
<b>4.1 General requirements</b>	
<b>4.2 Security management policy</b>	
<b>4.3 Security risk assessment and planning</b>	
<b>4.4 Implementation and operation</b>	
<b>4.5 Checking and corrective action</b>	
<b>4.6 Management review and continual improvement</b>	
<b>Annex A (informative) Correspondence between ISO/DIS28000, ISO14001 :2004 and ISO9001:2000</b>	
<b>Bibliography</b>	

## Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

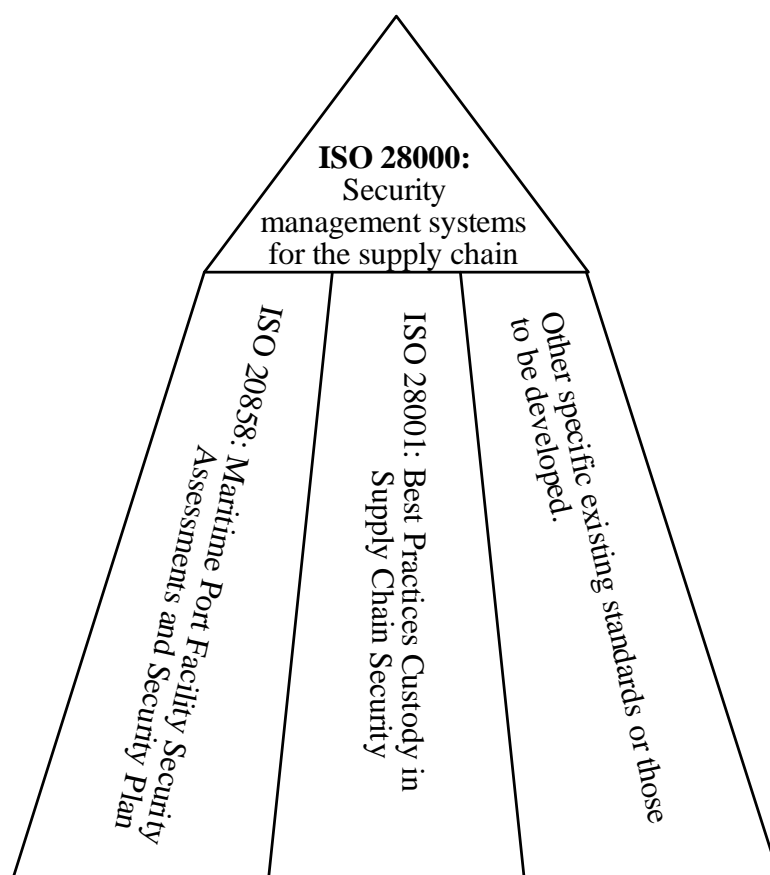
The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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

ISO 28000 was prepared by Technical Committee ISO/TC 8, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.

## Introduction

This Draft International Standard has been developed in response to demand from industry for a security management standard. Its ultimate objective is to improve the security of supply chains. This DIS is a high level management standard that enables an organization to establish an overall supply chain security management system. It requires the organization to assess the security environment in which it operates and to determine if adequate security measures are in place and if other regulatory requirements already exist with which the organization complies. If security needs are identified by this process, the organization should implement mechanisms and processes to meet these needs. Since supply chains are dynamic in nature, some organizations managing multiple supply chains may look to their service providers to meet related governmental or ISO supply chain security standards as a condition of being included in that supply chain in order to simplify security management as illustrated in Figure 1.



**Figure 1 – Relationship between ISO/DIS 28000 and other relevant standards**

This Standard is intended to apply in cases where an organization's supply chains are required to be managed in a secure manner. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

Compliance with a Standard does not in itself confer immunity from legal obligations. For organizations that so wish, compliance of the security management system to this Standard may be verified by an external or internal auditing process.

This Standard is based on the ISO format adopted by ISO 14001:2004 because of its risk based approach to management systems. However, organizations that have adopted a process approach to management systems (e.g. ISO 9001:2000) may be able to use their existing management system as a foundation for a security management system as prescribed in this Standard. It is not the intention of this Standard to duplicate governmental requirements and standards regarding supply chain security management to which the organization has already been certified or verified compliant. Verification may be by an acceptable first, second, or third party organization.

Note: This Standard is based on the methodology known as Plan-Do-Check-Act (PDCA). PDCA can be described as follows:

- Plan: establish the objectives and processes necessary to deliver results in accordance with the organization's security policy
- Do: implement the processes
- Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results
- Act: take actions to continually improve performance of the security management system

# Specification for security management systems for the supply chain

## 1. Scope

This Draft International Standard specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. Security management is linked to many other aspects of business management. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

This Draft International Standard is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

- a) establish, implement, maintain and improve a security management system;
- b) assure compliance with stated security management policy;
- c) demonstrate such compliance to others;
- d) seek certification/registration of its security management system by an Accredited third party Certification Body; or
- e) make a self-determination and self-declaration of compliance with this Specification.

There are legislative and regulatory codes that address some of the requirements in this DIS.

It is not the intention of this standard to require duplicative demonstration of compliance.

Organizations that choose third party certification can further demonstrate that they are contributing significantly to supply chain security.

## 2. Normative references

No normative references are cited. This clause is included in order to retain clause numbering similar to other management system standards.

### 3. Terms and Definitions

For the purposes of this DIS, the following terms and definitions apply:

- 3.1 Facility: plant, machinery, property, buildings, vehicles, ships, port facilities and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function or service.

NOTE: This definition includes any software code that is critical to the delivery of security and the application of security management.

- 3.2 Security: resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain.

- 3.3 Security management: systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts there from.

- 3.4 Security management objective: specific outcome or achievement required of security in order to meet the security management policy.

NOTE: It is essential that such outcomes are linked either directly or indirectly to providing the products, supply or services delivered by the total business to its customers or end users.

- 3.5 Security management policy: overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements.

- 3.6 Security management programmes: the means by which a security management objective is achieved.

- 3.7 Security management target: specific level of performance required to achieve a security management objective.

- 3.8 Stakeholder: person or entity having a vested interest in the organization's performance, success or the impact of its activities.

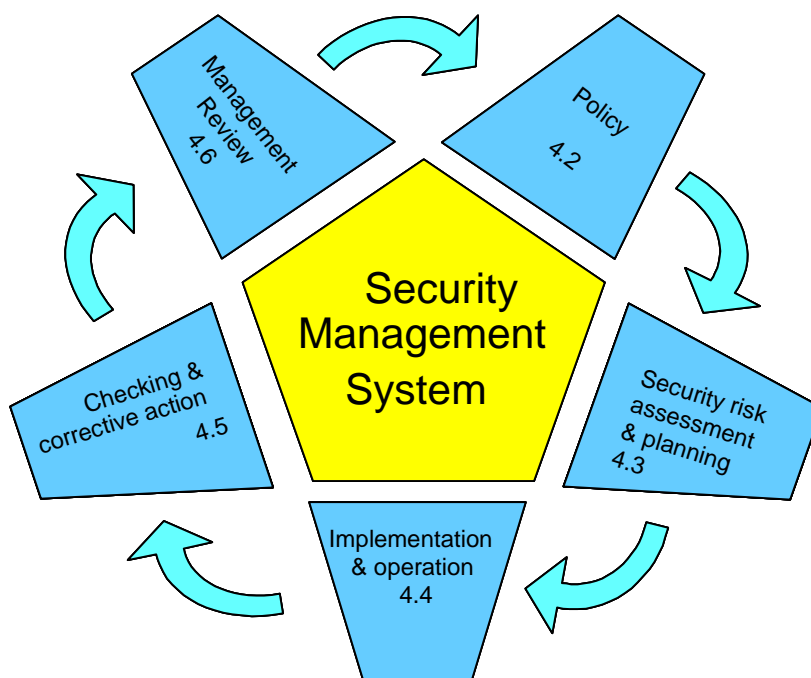
NOTE: Examples include customers, shareholders, financiers, insurers, regulators, statutory bodies, employees, contractors, suppliers, labour organizations, or society.

- 3.9 Supply chain: the linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities that lead to the end user.



- 3.9.1 Downstream: refers to the actions, processes and movements of the cargo in the supply chain that occur after the cargo leaves the direct operational control of the organization, including but not limited to insurance, finance, data management, and the packing, storing and transferring of cargo.
- 3.9.2 Upstream: refers to the actions, processes and movements of the cargo in the supply chain that occur before the cargo comes under the direct operational control of the organization. Including but not limited to insurance, finance, data management, and the packing, storing and transferring of cargo.
- 3.10 Top Management: person or group of people who directs and controls an organization at the highest level.
- NOTE: Top management, especially in a large multinational organization, may not be personally involved as described in the Specification; however top management accountability through the chain of command shall be manifest.
- 3.11 Continual Improvement: recurring process of enhancing the security management system in order to achieve improvements in overall security performance consistent with the organization's security policy.

#### 4. Security management system elements



**Figure 2 — Security management system elements**

## 4.1 General requirements

The organization shall establish, document, implement, maintain and continually improve an effective security management system for identifying security risks and controlling and mitigating their consequences.

The organization shall continually improve its effectiveness in accordance with the requirements set out in the whole of Clause 4.

The organization shall define the scope of its security management system. Where an organization chooses to outsource any process that affects conformity with these requirements, the organization shall ensure that such processes are controlled. The necessary controls and responsibilities of such outsourced processes shall be identified within the security management system.

## 4.2 Security management policy

The organization's top management shall authorize an overall security management policy. The policy shall:

- a) be consistent with other organizational policies;
- b) provide the framework which, enables the specific security management objectives, targets and programmes to be produced;
- c) be consistent with the organization's overall security threat and risk management framework;
- d) be appropriate to the threats to the organization and the nature and scale of its operations;
- e) clearly state the overall/broad security management objectives;
- f) include a commitment to continual improvement of the security management process;
- g) include a commitment to comply with current applicable legislation, regulatory and statutory requirements and with other requirements to which the organization subscribes;
- h) be visibly endorsed by top management;
- i) be documented, implemented and maintained;
- j) be communicated to all relevant employees and third parties including contractors and visitors with the intent that these persons are made aware of their individual security management-related obligations;
- k) be available to stakeholders where appropriate;

- l) provide for its review in case of the acquisition of, or merger with other organizations, or other change to the business scope of the organization which may affect the continuity or relevance of the security management system.

NOTE: Organizations may choose to have a detailed security management policy for internal use which would provide sufficient information and direction to drive the security management system (parts of which may be confidential) and have a summarized (non-confidential) version containing the broad objectives for dissemination to its stakeholders and other interested parties.

## 4.3 Security risk assessment and planning

### 4.3.1 Security risk assessment

The organization shall establish and maintain procedures for the ongoing identification and assessment of security threats and security management-related threats and risks, and the identification and implementation of necessary management control measures. Security threats and risk identification, assessment and control methods should, as a minimum, be appropriate to the nature and scale of the operations. This assessment shall consider the likelihood of an event and all of its consequences which shall include:

- a) physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action;
- b) operational threats and risks, including the control of the security, human factors and other activities which affect the organizations performance, condition or safety;
- c) natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective;
- d) factors outside of the organization's control, such as failures in externally supplied equipment and services;
- e) stakeholder threats and risks such as failure to meet regulatory requirements or damage to reputation or brand;
- f) design and installation of security equipment including replacement, maintenance, etc.
- g) information and data management and communications.
- h) a threat to continuity of operations

The organization shall ensure that the results of these assessments and the effects of these controls are considered and, where appropriate, provide input into:

- a) security management objectives and targets;

- b) security management programmes;
- c) the determination of requirements for the design, specification and installation;
- d) identification of adequate resources including staffing levels;
- e) identification of training needs and skills (see 4.4.2);
- f) development of operational controls (see 4.4.6);
- g) the organization's overall threat and risk management framework.

The organization shall document and keep the above information up to date.

The organization's methodology for threat and risk identification and assessment shall:

- a) be defined with respect to its scope, nature and timing to ensure it is proactive rather than reactive;
- b) include the collection of information related to security threats and risks;
- c) provide for the classification of threats and risks and identification of those that are to be avoided, eliminated or controlled;
- d) provide for the monitoring of actions to ensure effectiveness and the timeliness of their implementation (see 4.5.1).

### **4.3.2 Legal, statutory and other security regulatory requirements**

The organization shall establish, implement and maintain a procedure

- a) to identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks, and
- b) to determine how these requirements apply to its security threats and risks.

The organization shall keep this information up-to-date. It shall communicate relevant information on legal and other requirements to its employees and other relevant third parties including contractors.

### **4.3.3 Security management objectives**

The organization shall establish, implement and maintain documented security management objectives at relevant functions and levels within the organization. The objectives shall be derived from and consistent with the policy. When establishing and reviewing its objectives, an organization shall take into account:

- a) legal, statutory and other security regulatory requirements;

- b) security related threats and risks;
- c) technological and other options;
- d) financial, operational and business requirements;
- e) views of appropriate stakeholders.

The security management objectives shall be:

- a) consistent with the organization's commitment to continual improvement;
- b) quantified (where practicable);
- c) communicated to all relevant employees and third parties, including contractors, with the intent that these persons are made aware of their individual obligations;
- d) reviewed periodically to ensure that they remain relevant and consistent with the security management policy. Where necessary the security management objectives shall be amended accordingly.

#### **4.3.4 Security management targets**

The organization shall establish, implement and maintain documented security management targets appropriate to the needs of the organization. The targets shall be derived from and be consistent with the security management objectives.

These targets shall be:

- a) to an appropriate level of detail;
- b) specific, measurable, achievable, relevant and time-based (where practicable);
- c) communicated to all relevant employees and third parties including contractors with the intent that these persons are made aware of their individual obligations;
- d) reviewed periodically to ensure that they remain relevant and consistent with the security management objectives. Where necessary the targets shall be amended accordingly.

#### **4.3.5 Security management programmes**

The organization shall establish, implement and maintain security management programmes for achieving its objectives and targets.

The programmes shall be optimized and then prioritized, and the organization shall provide for the efficient and cost effective implementation of these programmes.

This shall include documentation which describes:

- a) the designated responsibility and authority for achieving security management objectives and targets;
- b) the means and time-scale by which security management objectives and targets are to be achieved.

The security management programmes shall be reviewed periodically to ensure that they remain effective and consistent with the objectives and targets. Where necessary the programmes shall be amended accordingly.

## **4.4 Implementation and operation**

### **4.4.1 Structure, authority and responsibilities for security management**

The organization shall establish and maintain an organizational structure of roles, responsibilities and authorities, consistent with the achievement of its security management policy, objectives, targets and programmes.

These roles, responsibilities and authorities shall be defined, documented and communicated to the individuals responsible for implementation and maintenance.

Top management shall provide evidence of its commitment to the development and implementation of the security management system (processes) and continually improving its effectiveness by:

- a) appointing a member of top management who, irrespective of other responsibilities, shall be responsible for the overall design, maintenance, documentation and improvement of the organization's security management system ;
- b) appointing (a) member(s) of management with the necessary authority to ensure that the objectives and targets are implemented;
- c) identifying and monitoring the requirements and expectations of the organization's stakeholders and taking appropriate and timely action to manage these expectations;
- d) ensuring the availability of adequate resources;
- e) considering the adverse impact that the security management policy; objectives, targets, programmes, etc. may have on other aspects of the organization;
- f) ensuring any security programmes generated from other parts of the organization complement the security management system;
- g) communicating to the organization the importance of meeting its security management requirements in order to comply with its policy;
- h) ensuring security-related threats and risks are evaluated and included in organizational threat and risk assessments, as appropriate;
- i) ensuring the viability of the security management objectives, targets and programmes.

#### 4.4.2 Competence, training and awareness

The organization shall ensure that personnel responsible for the design, operation and management of security equipment and processes are suitably qualified in terms of education, training and/or experience. The organization shall establish and maintain procedures to make persons working for it or on its behalf aware of:

- a) the importance of compliance with the security management policy and procedures, and to the requirements of the security management system;
- b) their roles and responsibilities in achieving compliance with the security management policy and procedures and with the requirements of the security management system, including emergency preparedness and response requirements;
- c) the potential consequences to the organization's security by departing from specified operating procedures.

Records of competence and training shall be kept.

#### 4.4.3 Communication

The organization shall have procedures for ensuring that pertinent security management information is communicated to and from relevant employees, contractors and other stakeholders.

Because of the sensitive nature of certain security related information, due consideration should be given to the sensitivity of information prior to dissemination.

#### 4.4.4 Documentation

The organization shall establish and maintain a security management documentation system that includes, but is not limited to the following:

- a) the security policy, objectives and targets
- b) description of the scope of the security management system,
- c) description of the main elements of the security management system and their interaction, and reference to related documents,
- d) documents, including records, required by this International Standard, and
- e) determined by the organization to be necessary to ensure the effective planning, operation and control of processes that relate to its significant security threats and risks.

The organization shall determine the security sensitivity of information and shall take steps to prevent unauthorized access.

#### **4.4.5 Document and data control**

The organization shall establish and maintain procedures for controlling all documents, data and information required by Clause 4 of this Specification to ensure that:

- a) these documents, data and information can be located and accessed only by authorized individuals;
- b) these documents, data and information are periodically reviewed, revised as necessary, and approved for adequacy by authorized personnel;
- c) current versions of relevant documents, data and information are available at all locations where operations essential to the effective functioning of the security management system are performed;
- d) obsolete documents, data and information are promptly removed from all points of issue and points of use, or otherwise assured against unintended use;
- e) archival documents, data and information retained for legal or knowledge preservation purposes or both are suitably identified;
- f) these documents, data and information are secure, and if in electronic form are adequately backed up and can be recovered.

#### **4.4.6 Operational control**

The organization shall identify those operations and activities that are necessary for achieving:

- a) its security management policy;
- b) the control of identified security threats and risks;
- c) compliance with legal, statutory and other regulatory security requirements;
- d) its security management objectives;
- e) the delivery of its security management programmes;
- f) the required level of supply chain security.

The organization shall ensure these operations and activities are carried out under specified conditions by:

- a) establishing, implementing and maintaining documented procedures to control situations where their absence could lead to failure to achieve the operations and activities listed in 4.4.6 a) to f) above;



- b) evaluating any threats posed from upstream supply chain activities and applying controls to mitigate these impacts to the organization and other downstream supply chain operators;
- c) establishing and maintaining the requirements for goods or services which impact on security and communicating these to suppliers and contractors.

These procedures shall include controls for the design, installation, operation, refurbishment, and modification of security related items of equipment, instrumentation, etc., as appropriate. Where existing arrangements are revised or new arrangements introduced, that could impact on security management operations and activities, the organization shall consider the associated security threats and risks before their implementation. The new or revised arrangements to be considered shall include:

- a) revised organizational structure, roles or responsibilities;
- b) revised security management policy, objectives, targets or programmes;
- c) revised processes and procedures;
- d) the introduction of new infrastructure, security equipment or technology, which may include hardware and/or software;
- e) the introduction of new contractors, suppliers or personnel, as appropriate.

#### **4.4.7 Emergency preparedness, response and security recovery**

The organization shall establish, implement and maintain appropriate plans and procedures to identify the potential for, and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them. The plans and procedures shall include information on the provision and maintenance of any identified equipment, facilities or services that can be required during or after incidents or emergency situations.

The organization shall periodically review the effectiveness of its emergency preparedness, response and security recovery plans and procedures, in particular after the occurrence of incidents or emergency situations caused by security breaches and threats. The organization shall periodically test these procedures where practicable.

### **4.5 Checking and corrective action**

#### **4.5.1 Security performance measurement and monitoring**

The organization shall establish and maintain procedures to monitor and measure the performance of its security management system. It shall also establish and maintain procedures to monitor and measure the security performance. The organization shall consider the associated security threats and risks, including potential deterioration mechanisms and their consequences, when setting the frequency for measuring and monitoring the key performance parameters. These procedures shall provide for:

- a) both qualitative and quantitative measurements, appropriate to the needs of the organization;

- b) monitoring the extent to which the organization's security management policy, objectives and targets are met;
- c) proactive measures of performance that monitor compliance with the security management programs, operational control criteria and applicable legislation, , statutory, and other security regulatory requirements;
- d) reactive measures of performance to monitor security-related deteriorations, failures, incidents, non-conformances (including near misses and false alarms) and other historical evidence of deficient security management system performance;
- e) recording data and results of monitoring and measurement sufficient to facilitate subsequent corrective and preventative action analysis. If monitoring equipment is required for performance and/or measurement and monitoring, the organization shall require the establishment and maintenance of procedures for the calibration and maintenance of such equipment. Records of calibration and maintenance activities and results shall be retained for sufficient time to comply with legislation and the organization's policy.

#### **4.5.2 System evaluation**

The organization shall evaluate security management plans, procedures, and capabilities capabilities through periodic reviews, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes in these factors must be reflected immediately in the procedure(s).

The organization shall periodically evaluate compliance with relevant legislation and regulations, industry best practices, and conformance with its own policy and objectives.

The organization shall keep records of the results of the periodic evaluations.

#### **4.5.3 Security-related failures, incidents, non-conformances and corrective and preventive action**

The organization shall establish, implement and maintain procedures for defining responsibility and authority for:

- a) evaluating and initiating preventive actions to identify potential failures of security in order that that may be prevented from occurring;
- b) the investigation of security-related:
  - i) failures including near misses and false alarms;
  - ii) incidents and emergency situations;
  - iii) non-conformances;
- c) taking action to mitigate any consequences arising from such failures, incidents or non-conformances;
- d) the initiation and completion of corrective actions;
- e) the confirmation of the effectiveness of corrective actions taken.

These procedures shall require that all proposed corrective and preventive actions are reviewed through the security threat and risk assessment process prior to implementation unless immediate implementation forestalls imminent exposures to life or public safety.

Any corrective or preventive action taken to eliminate the causes of actual and potential non-conformances shall be appropriate to the magnitude of the problems and commensurate with the security management-related threats and risks likely to be encountered. The organization shall implement and record any changes in the documented procedures resulting from corrective and preventive action and shall include the required training where necessary.

#### **4.5.4 Control of Records**

The organization shall establish and maintain records as necessary to demonstrate conformity to the requirements of its security management system and of this standard, and the results achieved.

The organization shall establish, implement and maintain a procedure(s) for the identification, storage, protection, retrieval, retention and disposal of records.

Records shall be and remain legible, identifiable and traceable.

Electronic and digital documentation should be rendered tamper proof, securely backed-up and accessible only to authorized personal.

#### 4.5.5 Audit

The organization shall establish, implement and maintain a security management audit program and shall insure that audits of the security management system are carried out at planned intervals, in order to:

- a) determine whether or not the security management system :
  - i) conforms to planned arrangements for security management including the requirements of the whole of Clause 4 of this specification;
  - ii) has been properly implemented and maintained;
  - iii) is (are) effective in meeting the organization's security management policy and objectives;
- b) review the results of previous audits and the actions taken to rectify non-conformances;
- c) provide information on the results of audits to management;
- d) verify that the security equipment and personnel are appropriately deployed.

The audit program, including any schedule, shall be based on the results of threat and risk assessments of the organization's activities, and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results. Where possible, audits shall be conducted by personnel independent of those having direct responsibility for the activity being examined.

NOTE: The phrase "personnel independent" does not necessarily mean personnel external to the organization.

#### 4.6 Management review and continual improvement

Top management shall review the organization's security management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. Reviews shall include assessing opportunities for improvement and the need for changes to the security management system, including the security policy and security objectives and threats and risks. Records of the management reviews shall be retained. Input to management reviews shall include

- a) results of audits and evaluations of compliance with legal requirements and with other requirements to which the organization subscribes,
- b) communication(s) from external interested parties, including complaints,
- c) the security performance of the organization,

- d) the extent to which objectives and targets have been met,
- e) status of corrective and preventive actions,
- f) follow-up actions from previous management reviews,
- g) changing circumstances, including developments in legal and other requirements related to its security aspects, and
- h) recommendations for improvement.

The outputs from management reviews shall include any decisions and actions related to possible changes to security policy, objectives, targets and other elements of the security management system, consistent with the commitment to continual improvement.

## Annex A

(Informative)

## Correspondence between ISO 28000:2005, ISO 14001:2004 and ISO 9001:2000

ISO 28000:2005		ISO 14001:2004		ISO 9001:2000	
Supply chain security management system requirements (title only)	4	Environmental management system requirements (title only)	4	Quality management system requirements (title only)	4
General requirements	4.1	General requirements	4.1	General requirements	4.1
Security management policy	4.2	Environmental policy	4.2	Management commitment	5.1
				Quality policy	5.3
				Continual improvement	8.5.1
Security risk assessment and planning (title only)	4.3	Planning (title only)	4.3	Planning (title only)	5.4
Security risk assessment	4.3.1	Environmental aspects	4.3.1	Customer focus	5.2
				Determination of requirements related to the product	7.2.1
				Review of requirements related to the product	7.2.2
Legal, statutory and other security regulatory requirements	4.3.2	Legal and other requirements	4.3.2	Customer focus	5.2
				Determination of requirements related to the product	7.2.1
Security management objectives,	4.3.3	Objectives, targets and programme(s)	4.3.3	Quality objectives	5.4.1
				Quality management system	

				planning	5.4.2
				Continual improvement	8.5.1
Security management targets	4.3.4	Objectives, targets and programme(s)	4.3.3	Quality objectives	5.4.1
				Quality management system planning	5.4.2
				Continual improvement	8.5.1
Security management programme(s)	4.3.5	Objectives, targets and programme(s)	4.3.3	Quality objectives	5.4.1
				Quality management system planning	5.4.2
				Continual improvement	8.5.1
Implementation and operation (title only)	4.4	Implementation and operation (title only)	4.4	Product realization (title only)	7
Structure, authority and responsibilities for security management	4.4.1	Resources, roles, responsibility and authority	4.4.1	Management commitment	5.1
				Responsibility and authority	5.5.1
				Management representative	5.5.2
				Provision of resources	6.1
				Infrastructure	6.3
Competence, training and awareness	4.4.2	Competence, training and awareness	4.4.2	(Human resources) General	6.2.1
				Competence, awareness and training	6.2.2
Communication	4.4.3	Communication	4.4.3	Internal communication	5.5.3
				Customer communication	7.2.3
Documentation	4.4.4	Documentation	4.4.4	(Documentation requirements) General	4.2.1
Document and data control	4.4.5	Control of documents	4.4.5	Control of documents	4.2.3

Operational control	4.4.6	Operational control	4.4.6	Planning of product realization Determination of requirements related to the product Review of requirements related to the product Design and development planning Design and development inputs Design and development outputs Design and development review Design and development verification Design and development validation Control of design and development changes Purchasing process Purchasing information Verification of purchased product Control of production and service provision Validation of processes for production and service provision Preservation of product	7.1 7.2.1 7.2.2  7.3.1 7.3.2 7.3.3 7.3.4 7.3.5  7.3.6 7.3.7  7.4.1 7.4.2 7.4.3 7.5.1  7.5.2  7.5.5
Emergency preparedness, response and security recovery	4.4.7	Emergency preparedness and response	4.4.7	Control of nonconforming product	8.3
Checking and corrective action (title only)	4.5	Checking (title only)	4.5	Measurement, analysis and improvement (title only)	8



Security performance measurement and monitoring	4.5.1	Monitoring and measurement	4.5.1	Control of monitoring and measuring devices  General (measurement, analysis and improvement)  Monitoring and measurement of processes  Monitoring and measurement of product  Analysis of data	7.6  8.1  8.2.3  8.2.4  8.4
System evaluation	4.5.2	Evaluation of compliance	4.5.2	Monitoring and measurement of processes  Monitoring and measurement of product	8.2.3  8.2.4
Security related failures, incidents, non conformances and corrective and preventive action	4.5.3	Nonconformity, corrective action and preventive action	4.5.3	Control of nonconforming product  Analysis of data  Corrective action  Preventive action	8.3  8.4  8.5.2  8.5.3
Control of records	4.5.4	Control of records	4.5.4	Control of records	4.2.4
Audit	4.5.5	Internal audit	4.5.5	Internal audit	8.2.2
Management review and continual improvement	4.6	Management review	4.6	Management commitment  Management review (title only)  General  Review input  Review output  Continual improvement	5.1  5.6  5.6.1  5.6.2  5.6.3  8.5.1

### Bibliography

- 1 ISO 9001:2000; Quality management systems— Requirements
- 2 ISO 14001:2004; Environmental management systems—Requirements with guidance for s
- 3 ISO 19011:2002; Guidelines for quality and/or environmental management systems auditing