INTERNATIONAL STANDARD

ISO 28004

First edition
2007-10-15

Security management systems for the supply chain — Guidelines for the implementation of ISO 28000

Systèmes de management de la sûreté pour la chaîne d'approvisionnement — Lignes directrices pour la mise en application de l'ISO 28000

Reference number
ISO 28004:2007(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 28004 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.

This first edition of ISO 28004 cancels and replaces ISO/PAS 28004:2006, which has been technically revised.

Introduction

ISO 28000:2007, *Specification for security management systems for the supply chain,* and this International Standard have been developed in response to the need for a recognizable supply chain management system standard against which their security management systems can be assessed and certified and for guidance on the implementation of such a standard.

ISO 28000 is compatible with the ISO 9001:2000 (Quality) and ISO 14001:2004 (Environmental) management systems standards. They facilitate the integration of quality, environmental and supply chain management systems by organizations, should they wish to do so.

This International Standard includes a box at the beginning of each clause/subclause, which gives the complete requirements from ISO 28000; this is followed by relevant guidance. The clause numbering of this International Standard is aligned with that of ISO 28000.

This International Standard will be reviewed or amended when considered appropriate. Reviews will be conducted when ISO 28000 is revised.

This International Standard does not purport to include all necessary provisions of a contract between supply chain operators, suppliers and stakeholders. Users are responsible for its correct application.

Compliance with this International Standard does not of itself confer immunity from legal obligations.

Security management systems for the supply chain — Guidelines for the implementation of ISO 28000

1 Scope

This International Standard provides generic advice on the application of ISO 28000:2007, *Specification for security management systems for the supply chain*.

It explains the underlying principles of ISO 28000 and describes the intent, typical inputs, processes and typical outputs, for each requirement of ISO 28000. This is to aid the understanding and implementation of ISO 28000.

This International Standard does not create additional requirements to those specified in ISO 28000, nor does it prescribe mandatory approaches to the implementation of ISO 28000.

ISO 28000

1 Scope

This 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 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 International Standard.

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

It is not the intention of this International 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 ISO 28000.

3 Terms and definitions

ISO 28000

3 Terms and definitions

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
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
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

NOTE The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centres, 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 this International Standard; 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

For the purposes of this document, the terms and definitions given in ISO 28000 and the following apply.

3.1
risk
likelihood of a security threat materializing and the consequences

3.2
security cleared
process of verifying the trustworthiness of people who will have access to security sensitive material

3.3
threat
any possible intentional action or series of actions with a damaging potential to any of the stakeholders, the facilities, operations, the supply chain, society, economy or business continuity and integrity

4 Security management system elements

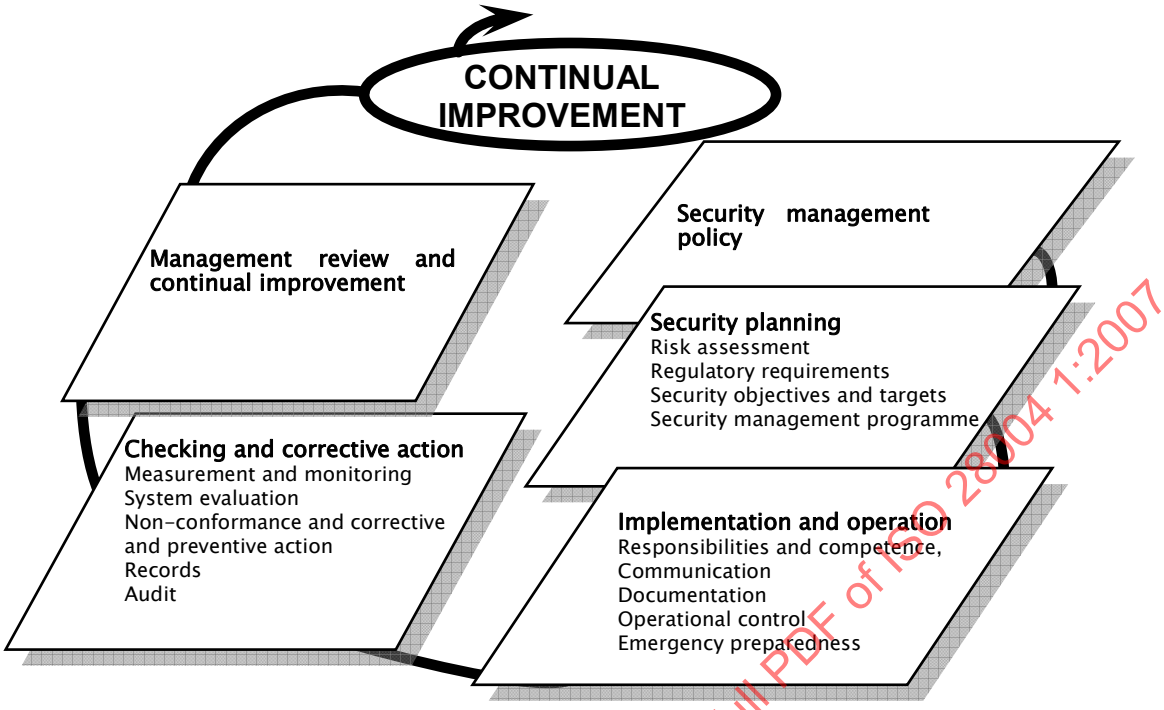

Figure 1 — Elements of successful security management

4.1 General requirements

a) ISO 28000 requirement

The organization shall establish, document, implement, maintain and continually improve an effective security management system for identifying security threats, assessing 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.

b) Intent

The organization should establish and maintain a management system that conforms to all of the requirements of ISO 28000. This may assist the organization in meeting security regulations, requirements and laws.

The level of detail and complexity of the security management system, the extent of documentation and the resources devoted to it are dependent on the size and complexity of an organization and the nature of its activities.

An organization has the freedom and flexibility to define its boundaries and may choose to implement ISO 28000 with respect to the entire organization or to specific operating units or activities of the organization.

Caution should be taken when defining the boundaries and scope of the management system. Organizations should not attempt to limit their scope so as to exclude from assessment, an operation or activity required for the overall operation of the organization or those that can impact on the security of its employees and other interested parties.

If ISO 28000 is implemented for a specific operating unit or activity, the security policies and procedures developed by other parts of the organization may be able to be used by the specific operating unit or activity to assist in meeting the requirements of ISO 28000. This may require that these security policies or procedures are subject to minor revision or amendment, to ensure that they are applicable to the specific operating unit or activity.

c) Typical input

All input requirements are specified in ISO 28000.

d) Typical output

A typical output is an effectively implemented and maintained security management system that assists the organization in continually seeking for improvements.

4.2 Security management policy

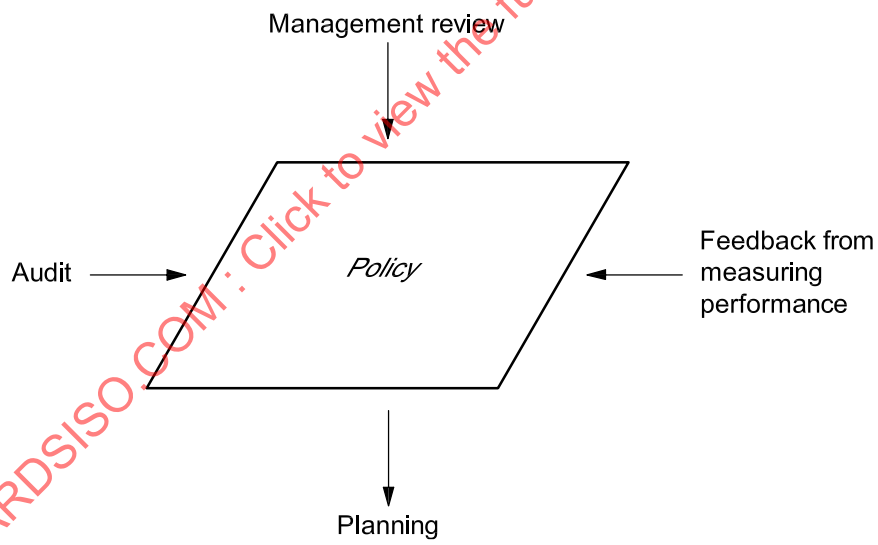

Figure 2 — Security management policy

a) ISO 28000 requirement

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.

b) Intent

A security policy is a concise statement of top management's commitment to security. A security policy establishes an overall sense of direction and sets the principles of action for an organization. It sets security objectives for security responsibility and performance required throughout the organization.

A documented security policy should be produced and authorized by the organization's top management.

c) Typical inputs

In establishing the security policy, management should consider the following items, especially in relation to its supply chain:

- policy and objectives relevant to the organization's business as a whole;
- historical and current security performance by the organization;
- needs of stakeholders;

- opportunities and needs for continual improvement;
- resources needed;
- contributions of employees;
- contributions of contractors, stakeholders and other external personnel.

d) Process

When establishing and authorizing a security policy, top management should take into account the points listed below.

An effectively formulated and communicated security policy should:

1) be appropriate to the nature and scale of the organization's security risks;

Threat identification, risk assessment and risk management are at the heart of a successful security management system and should be reflected in the organization's security policy.

The security policy should be consistent with a vision of the organization's future. It should be realistic and should neither overstate the nature of the risks the organization faces, nor trivialize them.

2) include a commitment to continual improvement;

Global security threats increase the pressure on organizations to reduce the risk of incidents in the supply chain. In addition to meeting legal, national and regulatory responsibilities, and other regulations and guidance prepared by organizations such as the World Customs Organization (WCO), the organization should aim to improve its security performance and its security management system, effectively and efficiently, to meet the needs of changing global trade, business and regulatory needs.

Planned performance improvement should be expressed in the security objectives (see 4.3.2) and managed through the security management programme (see 4.3.5) although the security policy statement may include broad areas for action.

3) include a commitment to at least conform to current applicable security regulations and with other requirements to which the organization subscribes;

Organizations are required to conform to applicable security regulatory requirements. The security policy commitment is a public acknowledgement by the organization that it has a duty to conform to, if not exceed, any legislation, or other requirements, either legally mandated or adopted voluntarily subscribed to, such as the WCO SAFE Framework of Standards.

NOTE "Other requirements" can mean, for example, corporate or group policies, the organization's own internal standards or specifications or codes of practice to which the organization subscribes.

4) be documented, implemented and maintained;

Planning and preparation are the key to successful implementation. Often, security policy statements and security objectives are unrealistic because there are inadequate or inappropriate resources available to deliver them. Before making any public declarations the organization should ensure that any necessary finance, skills and resources are available and that all security objectives are realistically achievable within this framework.

In order for the security policy to be effective, it should be documented and be periodically reviewed for continuing adequacy and amended or revised if needed.

5) be communicated to all employees with the intent that employees are made aware of their individual security obligations;

The involvement and commitment of employees is vital for successful security.

Employees need to be made aware of the effects of security management on the quality of their own work environment and should be encouraged to contribute actively to security management.

Employees (at all levels, including management levels) are unlikely to be able to make an effective contribution to security management unless they understand the organization's policy and their responsibilities and are competent to perform their required tasks.

This requires the organization to communicate its security policies and security objectives to its employees clearly, to enable them to have a framework against which they can measure their own individual security performance.

6) be available to stakeholders;

Any individual or group (either internal or external) concerned with or affected by the security performance of the organization would be particularly interested in the security policy statement. Therefore, a process should exist to communicate the security policy to them. The process should ensure that stakeholders receive the security policy where appropriate.

7) be reviewed periodically to ensure that it remains relevant and appropriate to the organization.

Change is inevitable, regulations and legislation evolve and stakeholders' expectations increase. Consequently, the organization's security policy and management system needs to be reviewed regularly to ensure their continuing suitability and effectiveness.

If changes are introduced, these should be communicated as soon as practicable.

e) Typical output

A typical output is a comprehensive, concise, understandable, security policy that is communicated throughout the organization and to stakeholders as necessary.

4.3 Security risk assessment and planning

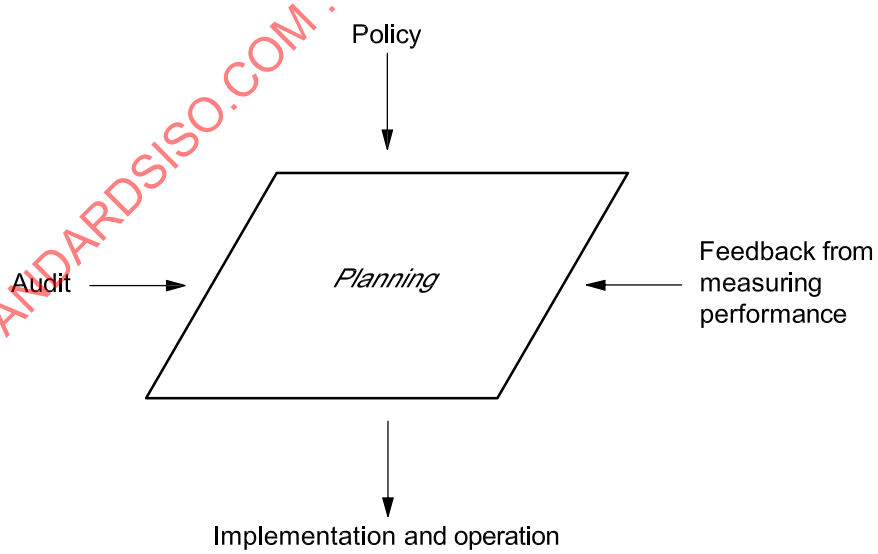

Figure 3 — Planning

4.3.1 Security risk assessment

a) ISO 28000 requirement

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).

b) Intent

The organization should have a total appreciation of significant security risk, threats and vulnerabilities in its domain, after using the processes of security threat identification, risk assessment and risk management.

The security threat identification, risk assessment and risk management processes and their outputs should be the basis of the whole security system. It is important that the links between the security threat identification, risk assessment and risk management processes and the other elements of the security management system are clearly established and apparent.

The purpose of this guideline is to establish principles by which the organization can determine whether or not given security threat identification, risk assessment and risk management processes are suitable and sufficient. It is not the purpose to make recommendations on how these activities should be conducted.

The security threat identification, risk assessment and risk management processes should enable the organization to identify, evaluate and control its security risks on an ongoing basis.

In all cases, consideration should be given to normal and abnormal operations within the organization and to potential emergency conditions.

The complexity of security threat identification, risk assessment and risk management processes greatly depends on factors such as the size of the organization, the workplace situations within the organization and the nature, complexity and significance of the security risk. It is not the purpose of ISO 28000:2007 **4.3.1**, to force small organizations with very limited security risk to undertake complex security threat identification, risk assessment and risk management exercises.

The security threat identification, risk assessment and risk management processes should take into account the cost and time of performing these three processes and the availability of reliable data. Information already developed for regulatory or other purposes may be used in these processes. The organization may also take into account the degree of practical control it can have over the security threats being considered. The organization should determine what its security threats are, taking into account the inputs and outputs associated with its current and relevant past activities, processes, products and /or services.

The security risk assessment should be conducted by qualified personnel using recognized methodologies which can be documented.

An organization with no existing security management system can establish its current position with regard to security risks by means of a risk assessment. The aim should be to consider security threats faced by the organization, as a basis for establishing the security management system. An organization should consider including (but not limiting itself to) the following items within its initial review:

- legislative and regulatory requirements;
- identification of the security threats faced by the organization;
- seeking security threat and risk information from appropriate policing and intelligence organizations;
- an examination of all existing security management practices, processes and procedures;
- an evaluation of feedback from the investigation of previous incidents and emergencies.

A suitable approach to the assessment can include checklists, interviews, direct inspection and measurement, results of previous management system audits or other reviews depending on the nature of the activities. All these activities should follow a documented repeatable methodology.

It is emphasized that an initial review is recommended to create a base line but is not a substitute for the implementation of the structured systematic approach given in the rest of **4.3.1**.

c) Typical inputs

Typical inputs include the following items:

- security legal and other requirements (see **4.3.2**);
- security policy (see **4.2**);
- records of incidents;
- non-conformances (see **4.5.3**);
- security management system audit results (see **4.5.5**);
- communications from employees and other interested parties (see **4.4.3**);
- information from employee security consultations, review and improvement activities in the workplace (these activities can be either reactive or proactive in nature);
- information on best practices, typical security risk related to the organization, incidents and emergencies having occurred in similar organizations;
- industry standards;
- government warnings;
- information on the facilities, processes and activities of the organization, including the following:
  - details of change control procedures;
  - site plan(s);
  - process manuals and operational procedures;
  - security data;
  - monitoring data (see **4.5.1**).

d) Process

1) *Security threat identification, risk assessment and risk management*

i) *General*

Measures for the management of risk should reflect the principle of the eliminating or reducing to a practicable minimum security risk, where practicable, either by reducing the likelihood of occurrence or the potential severity of impacts from security related incidents. Security threat identification, risk assessment and risk management processes are key tools in the management of risk.

Security threat identification, risk assessment and risk management processes vary greatly across industries, ranging from simple assessments to complex quantitative analyses with extensive documentation. It is for the organization to plan and implement appropriate security threat identification, risk assessment and risk management processes that suit its needs and its workplace situations and to assist it to conform to any security legislative requirements.

Security threat identification, risk assessment and risk management processes should be carried out as proactive measures, rather than as reactive ones, i.e. they should precede the introduction of new or revised activities or procedures. Any necessary risk reduction and control measures that are identified should be implemented before the changes are introduced.

The organization should keep its methodology, personnel qualifications, documentation, data and records concerning threat identification, risk assessment and risk management up-to-date in respect of ongoing activities and also extend them to consider new developments and new or modified activities, before these are introduced.

Security threat identification, risk assessment and risk management processes should not only be applied to "normal" operations of facility and procedures, but also to periodic or occasional operations/procedures.

As well as considering the security risk and risks posed by activities carried out by its own personnel, the organization should consider security risk and risks arising from the activities of contractors and visitors and from the use of products or services supplied to it by others.

ii) *Processes*

The security threat identification, risk assessment and risk management processes should be documented and should include the following elements:

- identification of security threats;
- evaluation of risks with existing (or proposed) control measures in place (taking into account exposure to specific security threats, the likelihood of failure of the control measures and the potential severity of consequences of injury, damage and operational continuity);
- evaluate the tolerability of current and residual risk;
- identification of any additional risk management measures needed;
- evaluation of whether the risk management measures are sufficient to reduce the risk to a tolerable level.

Additionally, the processes should address the following:

— the nature, timing, scope and methodology for any form of security threat identification, risk assessment and risk management that is to be used;

— applicable security legislation or other requirements;

— the roles and authorities of personnel responsible for performing the processes;

— the competency requirements and training needs (see **4.4.2**) for personnel who are to perform the processes. (Depending on the nature or type of processes to be used, it may be necessary for the organization to use external advice or services);

— the use of information from employee security inputs, reviews and improvement activities (these activities can be either reactive or proactive in nature).

iii) *Subsequent actions*

Following the performance of the security threat identification, risk assessment and risk management processes:

— there should be clear evidence that any corrective or preventive actions (see **4.5.2**) identified as being necessary are monitored for their timely completion (these may require that further security threat identification and risk assessments be conducted, to reflect proposed changes to risk management measures and to determine revised estimates of the residual risks);

— feedback on the results and on progress in the completion of corrective or preventive actions, should be provided to management, as input for management review (see **4.6**) and for the establishment of revised or new security objectives;

— the organization should be in a position to determine whether the competency of personnel performing specific security tasks is consistent with that specified by the risk assessment process in establishing the necessary risk management;

— feedback from subsequent operating experience should be used to amend the processes or the data on which they are based, as applicable.

2) *After the initial evaluation of security threat identification, risk assessment and risk managements (see also 4.6)*

The security threat identification, risk assessment and risk management process should be reviewed at a pre-determined time or period as set out in the security policy document or at a time pre-determined by management which may form part of the management review process (see 4.6). This period can vary depending on the following considerations:

- the nature of the security threats;
- the magnitude of the risk;
- changes from normal operation.

The review should also take place if changes within the organization call into question the validity of the existing assessments. Such changes can include the following elements:

- expansion, contraction, restructuring, changes to facilities or aspects of the supply chain;
- reapportioning of responsibilities;
- changes to methods of working or patterns of behaviour of security threats from outside sources.

e) Typical outputs

There should be documented procedure(s) for the following elements:

- identification of security threats;
- determination of the risks associated with the identified security threats;
- indication of the level of the risks related to each security threat and whether they are or are not, tolerable;
- description of or reference to, the measures to monitor and control the risks (see **4.4.6** and **4.5.1**), particularly risks that are not tolerable;
- where appropriate, the security objectives and actions to reduce identified risks (see **4.3.3**) and any follow-up activities to monitor progress in their reduction;
- identification of the competency and training requirements to implement the control measures (see **4.4.2**);
- necessary control measures detailed as part of the operational control element of the system (**4.4.6**);
- records generated by each of the above mentioned procedures.

4.3.2 Legal, statutory and other security regulatory requirements

a) ISO 28000 requirement

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.

b) Intent

The organization needs to be aware of and understand how its activities are or will be, affected by applicable legal and other requirements and to communicate this information to relevant personnel.

This requirement of **4.3.2** from ISO 28000:2007 is intended to promote awareness and understanding of legal and regulatory responsibilities. It is not intended to require the organization to establish libraries of legal or other documents that are rarely referenced or used.

c) Typical inputs

Typical inputs include the following items:

- details of the organization's supply chain;
- security threat identification, risk assessment and risk management results (see **4.3.1**);
- best practices (e.g. codes, industry association guidelines);
- legal requirements, governmental, intergovernmental, trade associations, codes and practices and regulations;
- listing of information sources;
- national, regional or international standards;
- internal organizational requirements;
- requirements of stakeholders;
- processes to manage the dynamics of the supply chain.

d) Process

Relevant legislation and other requirements should be identified. Organizations should identify the most appropriate means for accessing the information, including the media supporting the information (e.g. paper, CD, disk, internet). The organization should also evaluate which requirements apply and where they apply and who needs to receive the information.

e) Typical outputs

Typical outputs include the following items:

- procedures for identifying and accessing information and keeping it up to date;
- identification of which requirements apply and where [this can take the form of a register(s)];
- requirements (actual text, summary or analysis, where appropriate), available in locations which are to be decided by the organization;
- procedures for monitoring the implementation of controls consequent to new security legislation.

4.3.3 Security management objectives

a) ISO 28000 requirement

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.

b) Intent

It is necessary to ensure that, throughout the organization (where practical), measurable security objectives are established consistent with the security policy.

c) Typical inputs

Typical inputs include the following items:

- policy and objectives relevant to the organization's business as a whole;
- security policy, including the commitment to continual improvement (see **4.2**);
- results of security threat identification, risk assessment and risk management (see **4.3.1**);

- legal and other requirements (see **4.3.2**);
- technological options;
- financial, operational and business requirements;
- employees and stakeholder concerns (see **4.4.3**);
- information from employee security inputs, assessments and improvement activities in the workplace (these activities can be either reactive or proactive in nature);
- analysis of established security objectives;
- past records of security non-conformances, incidents and property damage;
- results of the management review (see **4.6**).

d) Process

Using information or data from inputs, appropriate management should identify, establish and prioritize security objectives.

During the establishment of security objectives, particular regard should be given to information or data from those most likely to be affected by individual security objectives, as this can assist in ensuring that they are reasonable and more widely accepted. It is also useful to consider information or data from sources external to the organization, e.g. from contractors, suppliers, business partners, police and intelligence agencies or stakeholders.

Meetings by the appropriate levels of management for the establishment of security objectives should be held regularly (e.g. at least on an annual basis). For some organizations, there can be a need to document the process of establishing the security objectives.

The security objectives should address both broad corporate security issues and security issues that are specific to supply chain(s), individual functions and levels within the organization.

Suitable indicators should be defined for each security objective, where practicable. These indicators should allow for the monitoring of the implementation of the security objectives.

Security objectives should be reasonable and achievable, in so much that the organization should have the ability to reach them and monitor progress. A reasonable and achievable time scale should be defined for the realization of each security objective.

Security objectives may be broken down into separate goals, depending on the size of the organization, the complexity of the security objective and its time-scale. There should be clear links between the various levels of goals and security objectives.

Examples of types of security objectives include:

- reduction of risk levels;
- the introduction of additional features into the security management system;
- the steps taken to improve existing facilities;
- the elimination or the reduction in frequency of particular undesired incident(s).

The security objectives should be communicated (e.g. via training or group briefing sessions; see **4.4.2**) to relevant personnel and be deployed through the security management programme(s) (see **4.3.4**).

e) Typical outputs

Typical outputs include documented, measurable where practicable, security objectives for each function in the organization.

4.3.4 Security management targets

a) ISO 28000 requirement

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.

b) Intent

Security targets are set to achieve the objective within the specified time frame.

c) Typical inputs

- policy and objectives relevant to the organization's business as a whole;
- security policy, including the commitment to continual improvement (see **4.2**);
- results of security threat identification, risk assessment and risk management (see **4.3.1**);
- legal and other requirements (see **4.3.2**);
- technological options;
- financial, operational and business requirements;
- employees and stakeholder concerns (see **4.4.3**);
- information from employee security inputs, assessments and improvement activities in the workplace (these activities can be either reactive or proactive in nature);
- analysis of established security objectives;
- past records of security non-conformances and incidents;
- results of the management review (see **4.6**).

d) Process

The process is defined in the security programmes and is the achievable goals to meet the objective(s).

Using information or data from inputs, appropriate management should identify, establish and prioritize security targets. The targets should be specific, time based and measurable.

During the establishment of security targets, particular regard should be given to information or data from those most likely to be affected by individual security targets, as this can assist in ensuring that they are reasonable and more widely accepted. It is also useful to consider information or data from sources external to the organization, e.g. from contractors, suppliers, business partners, police and intelligence or stakeholders.

Meetings by the appropriate levels of management for establishing security targets should be reviewed after modification of the security objective. For some organizations, there can be a need to document the process of establishing the security targets.

The security targets should address both broad corporate security issues and security issues that are specific to supply chain(s), individual functions and levels within the organization.

Suitable indicators should be defined for each security target. These indicators should allow for the monitoring of the implementation of the security targets.

Security targets should be reasonable and achievable, in that the organization should have the ability to reach them and monitor progress. A reasonable and achievable time scale should be defined for the realization of each security target.

Security targets may be broken down into separate goals, depending on the size of the organization, the complexity of the security target and its time-scale. There should be clear links between the various levels of goals and security targets.

Examples of types of security targets include:

- reduction of risk levels within a given timeframe;
- the introduction of new technologies to reduce risk or mitigate impacts from security threats;
- the steps taken to improve existing facilities and their timeframe;
- the elimination or the reduction in frequency of particular undesired incident(s).

The security targets should be communicated (e.g. via training or group briefing sessions; see **4.4.2**) to relevant personnel and be deployed through the security management programme(s) (see **4.3.4**).

e) Typical outputs

Typical outputs include documented, measurable where practicable, security targets for each function in the organization.

4.3.5 Security management programmes

a) ISO 28000 requirement

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.

b) Intent

The security management programmes should be linked directly to the objectives and targets. Each management programme should describe how the organization will translate its goals and policy commitments into defined actions so that security objectives and targets are achieved. The programme will require the development of strategies and plans of actions to be taken, which should be documented and communicated. Progress of the programme with regard to meeting the stated objective(s) should be monitored, reviewed and recorded. The deterrence and mitigation strategy of the programme should be based on the results from security management threat and hazard identification and risk assessment, (such as: impact analysis, programme assessment, operational experience).

c) Typical inputs

Typical inputs include the following items:

- security objectives and targets;
- legal and other requirements;
- results of security threat identification, risk assessment and risk management;
- details of the organization's operations;
- information from employee security input, review and improvement activities in the workplace (these activities can be either reactive or proactive in nature);
- reviews of opportunities available from new or different technological options;
- continual improvement activities;
- availability of resources needed to achieve the organization's security objectives.

d) Process

The security management programme should define:

- the responsibilities for achieving goals;
- the means for achieving goals;
- the time frame for achieving those goals.

The programme should consider mitigating the threats through methodological and technological options and the experience of other entities while taking into account financial, operational and business requirements as well as the views of partner organizations and stakeholders.

It should provide for the allocation of appropriate responsibility and authority for each task and allocate time-scales to each individual task, in order to meet the overall time-scale of the related security objective. It should also provide for the allocation of suitable resources (e.g. financial, human, equipment, logistics) to each task.

Where significant alterations or modifications in working practices, processes, equipment or facilities are expected, the programme should provide for new security threat identification and risk assessment exercises. The security management programme should provide for consultation of relevant personnel on expected changes.

e) Typical outputs

Typical outputs include defined, documented security management programme(s) for achieving the objectives and targets describes in 4.3.3 and 4.3.4.

4.4 Implementation and operation

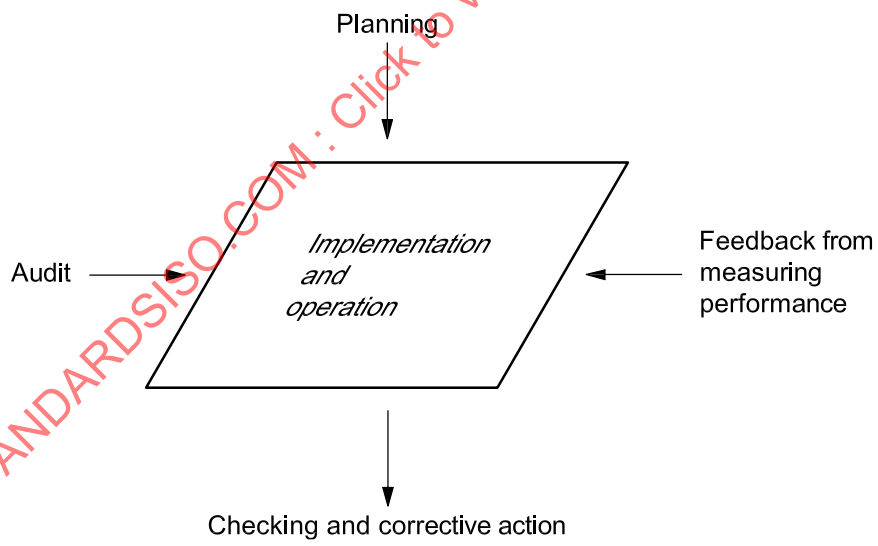

Figure 4 — Implementation and operation

4.4.1 Structure, authority and responsibilities for security management

a) ISO 28000 requirement

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.

b) Intent

To facilitate effective security management it is necessary that roles, responsibilities and authorities are defined, documented and communicated. Only security cleared staff (see definition in Clause 3) should be utilized for security critical tasks. Adequate resources should be provided to enable security tasks to be performed.

c) Typical inputs

Typical inputs include the following:

- organizational structure;
- security risk identification, risk assessment and risk control results;
- security objectives, targets and programmes;

- legal and other requirements;
- job descriptions;
- listings of qualified security personnel who need and/or have received security clearance.

d) Process

1) *Overview*

The responsibilities and authority of all persons who perform duties that are part of the security management system should be defined, including clear definitions of responsibilities at the interfaces between different functions.

Such definitions can, amongst others, be required for the following categories of people:

- top management;
- line management at all levels in the organization;
- those responsible for contractors and visitors which have access to the premises and its employees;
- those responsible for security training;
- those responsible for equipment and operations which are critical for security;
- employees with security clearances or other security specialists, within the organization;
- employee security representatives on consultative forums.

However, the organization should communicate and promote the idea that security is the responsibility of everyone in the organization, not just the responsibility of those with defined security management system duties.

2) *Defining top management responsibilities*

The responsibility of top management should include defining the organization's security policy and ensuring that the security management system is implemented. As part of this commitment, a specific management representative with defined responsibilities and authority for implementing the security management system should be designated and appointed by top management. (In large or complex organizations there may be more than one designated representative.)

3) *Defining security management representative responsibilities*

The security management representative should have the responsibility and authority for ensuring the security management system is implemented and documented, have ongoing access to top management and be supported by other personnel who have delegated responsibilities for monitoring the overall operation of the security function. The management representative should be regularly informed of the performance of the system and should retain active involvement in periodic reviews and the setting of security objectives. It should be ensured that any other duties or functions assigned to these personnel do not conflict with the fulfilment of their security responsibilities.

4) *Defining line management responsibilities*

Line management responsibility should include ensuring that security is managed within their area of operations. Where prime responsibility for security matters rests with line management, the role and responsibilities of any specialist security function within the organization should be appropriately defined to avoid ambiguity with respect to responsibilities and authorities. This should include arrangements to resolve any conflict between security issues and productivity considerations by escalation to a higher level of management.

5) *Documentation of roles and responsibilities*

Security responsibilities and authorities should be documented in a form appropriate to the organization. This can take one or more of the following forms or an alternative of the organization's choosing:

- security management system manuals;
- working procedures and task descriptions;
- job descriptions;
- induction training package and awareness programmes.

If the organization chooses to issue written job descriptions covering other aspects of employees' roles and responsibilities, then security responsibilities should be incorporated into those job descriptions.

6) *Communication of roles and responsibilities*

Security responsibilities and authorities should be appropriately communicated to those whom they affect within the organization. This should ensure that individuals understand the scope and the interfaces between the various functions and the channels to be used to initiate action.

7) *Resources*

Management should ensure that adequate resources are available for the maintenance of a secure supply chain, including equipment, human resources, expertise and training.

Resources can be considered adequate if they are sufficient to carry out security programmes and activities, including performance measurement and monitoring.

For organizations with established security management systems, the adequacy of resources can be at least partially evaluated by comparing the planned achievement of security objectives with actual results.

8) *Management commitment*

Managers should provide visible demonstration of their commitment to security. Means of demonstration can include visiting and inspecting sites, participating in security incident investigation and providing resources in the context of corrective action, attendance at security meetings and issuing messages of support.

e) Typical outputs

Typical outputs include the following:

- definitions of security responsibilities and authorities for all relevant personnel;
- documentation of roles/responsibilities in manuals/procedures/training packages;
- process for communicating roles and responsibilities to all employees and other relevant parties;
- active management participation and support for security, at all levels.

4.4.2 Competence, training and awareness

a) ISO 28000 requirement

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.

b) Intent

Organizations should have effective procedures for ensuring that personnel are competent to carry out their designated security functions and to be aware of security risks.

c) Typical inputs

Typical inputs include the following items:

- definitions of roles and responsibilities;
- job descriptions (including details of security tasks to be performed);
- employee performance appraisals;
- security risk identification, risk assessment and risk control results;
- procedures and operating instructions;
- security policy and security objectives;
- security programmes.

d) Process

The following elements should be included in the process:

- a systematic identification of the security awareness and competencies required at each level and function within the organization;
- arrangements to identify and remedy any shortfalls between the level currently possessed by the individual and the required security awareness and competency;
- provision of any training identified as being necessary, in a timely and systematic manner;

- assessment of individuals to ensure that they have acquired and that they maintain, the knowledge and competency required;
- maintenance of appropriate records of an individual's training and competency.

NOTE Strong emphasis on security awareness across the entire organization is important to a successful security management system and its effective implementation.

A security awareness and training programme should be established and maintained to address the following areas:

- ongoing awareness of security risks and threats;
- an understanding of the organization's security arrangements and individuals' specific roles and responsibilities;
- a systematic programme of induction and ongoing training for employees and those who transfer between divisions, sites, departments, areas, jobs or tasks within the organization;
- training in local security arrangements and security risk, risks, precautions to be taken and procedures to be followed, this training being provided before work commences;
- training for performing security risk identification, risk assessment and risk control (see **4.3.1d**);
- specific in-house or external training which can be required for employees with specific roles in the security system, including employee security representatives;
- training for all individuals who manage employees, contractors and others (e.g. temporary workers), in their security responsibilities. This is to ensure that both they and those under their control understand the security threats and risks of the operations for which they are responsible, wherever they take place. Additionally, this is to ensure that personnel have the competencies necessary to carry out the activities safely, by following security procedures;
- the roles and responsibilities (including corporate and individual legal responsibilities) of top management for ensuring that the security management system functions to control risks and minimize illness, injury and other losses to the organization;
- training and awareness programmes for contractors, temporary workers and visitors, according to the level of risk to which they are exposed.

The effectiveness of training and awareness programmes should be evaluated. This can involve assessment as part of the training exercise and/or appropriate field checks to establish whether competency and sufficient awareness has been attained or to monitor the longer term impact of training delivered.

e) Typical outputs

Typical outputs include the following items:

- competency requirements for individual roles;
- analysis of training needs;
- training programmes/plans;
- range of training courses/products available for use within the organization;
- training records and records of evaluation of the effectiveness and of training;
- security awareness programmes;
- evaluation of security awareness.

4.4.3 Communication

a) ISO 28000 requirement

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.

b) Intent

The organization should encourage participation in good security practices and support for its security policy and security objectives, from all those affected by its operations through a process of consultation and communication.

c) Typical inputs

Typical inputs include the following items:

- security policy and security objectives;
- relevant security management system documentation;
- security risk identification, risk assessment and risk control procedures;
- definitions of security roles and responsibilities;
- results of formal and informal employee security consultations with management;
- training programme details;
- relevant information from outside sources.

d) Process

The organization should document and promote the arrangements by which it consults on and communicates pertinent security information to and from its employees and other interested parties (e.g. contractors, visitors, stakeholders, business partners, authorities).

This should include arrangements to involve employees in the following processes:

- consultation over the development and review of policies, the development and review of security objectives and decisions on the implementation of processes and procedures to manage risks, including carrying out of security risk assessments and risk controls relevant to their own activities;
- consultation over changes affecting workplace security such as the introduction of new or modified, equipment, facilities, chemicals, technologies, processes, procedures or work patterns.

Employees should be encouraged to comment on security matters and should be informed of the specified management chain of command for security.

e) Typical outputs

Typical outputs include the following:

- formal management and employee consultations through security councils or similar bodies;
- employee involvement in security risk identification, risk assessment and risk control;
- initiatives to encourage employee security consultations, review and improvement activities in the workplace and feedback to management on security issues;
- employee security representatives with defined roles and communication mechanisms with management, including, for example, involvement in accident and incident investigations, site security inspections etc.;
- security briefings for employees and other interested parties, e.g. contractors or visitors;
- notice boards containing security information;
- security newsletter;
- security poster programme;
- other means for sharing sensitive security information and reports with appropriate authorities and supply chain partners.

4.4.4 Documentation

a) ISO 28000 requirement

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.

b) Intent

The organization should document and maintain up-to-date documentation to ensure that its security management system can be understood and effectively implemented and operated.

c) Typical inputs

Typical inputs include the following items:

- details of the documentation and information systems the organization develops to support its security management system and security activities and to fulfil the requirements of ISO 28000;
- responsibilities and authorities;
- information about facilities in which documentation or information is used and constraints that this can put on the physical nature of documentation or the use of electronic or other media.

d) Process

The organization should identify the data and information that is needed for the security management system, before developing the documentation necessary to support its security processes and security management system.

There is no requirement to develop documentation in a particular format in order to conform to ISO 28000, nor is it necessary to replace existing documentation such as manuals, procedures or work instructions if these adequately describe current arrangements. If the organization already has an established, documented security management system, it can prove more convenient and effective for it to develop, for example, a cross-reference document describing the inter-relation between its existing procedures and the requirements of ISO 28000.

Account should be taken of the following:

- the responsibilities and authorizations of the users of the documentation and information, as this should lead to determining the degree of security and accessibility that should be imposed;
- the manner in which physical documentation is used and the environment in which it is used. Similar consideration should be given concerning the use of electronic equipment for information systems.

e) Typical outputs

Typical outputs include the following items:

- security management system documentation overview document;
- document registers, master lists or indexes;
- procedures;
- work instructions.

4.4.5 Document and data control

a) ISO 28000 requirement

The organization shall establish and maintain procedures for controlling all documents, data and information required by Clause 4 of this International Standard 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.

b) Intent

All documents and data containing information critical to the operation of the security management system and the performance of the organization's security activities, should be identified and controlled.

c) Typical inputs

Typical inputs include the following items:

- details of the documentation and data systems the organization develops to support its security management system and security activities and to fulfil the requirements of ISO 28000;
- details of responsibilities and authorities.

d) Process

Written procedures should define the controls for the identification, approval, issue, access and removal of security documentation, together with the control of security of data. These procedures should clearly define the categories of documentation and data to which they apply and the level of classification based on security sensitivity.

Documentation and data should be available and accessible to authorized personnel when required, under routine and non-routine conditions, including emergencies.

e) Typical outputs

Typical outputs include the following items:

- document control procedure, including assigned responsibilities and authorities;
- document registers, master lists or indexes;
- list of controlled documentation and its location;
- archive records.

4.4.6 Operational control

a) ISO 28000 requirement

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 theses 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.

b) Intent

The organization should establish and maintain arrangements to ensure the effective application of control and counter measures, wherever these are required to control operational security risks, fulfil the security policy and objectives, achieve security targets and conform to legal and other requirements.

c) Typical inputs

Typical inputs include the following items:

- security policy and security objectives;
- security threat identification and risk assessment results;
- identified legal, regulatory and other requirements.

d) Process

The organization should establish procedures to control its identified risks (including those that could be introduced by contractors, other supply chain business partners or visitors), documenting these in instances where a failure to do so could lead to incidents, emergencies or other deviations from the security policy and security objectives. The risk management procedures should be reviewed on a regular basis for their suitability and effectiveness and changes that are identified as being necessary should be implemented.

Procedures should take account of situations where the risks extend to clients' or other external parties' premises or areas of control in other parts of the supply chain; for example, when employees of the organization are working at a client's site. It can sometimes be necessary to enter into consultation with the external party on security in such circumstances.

Some examples of areas in which risks typically arise and some examples of control measures against them are given below.

1) *Purchase or transfer of goods and services and use of external resources*

This includes for instance the following items:

- evaluation and periodic re-evaluation of the security competence of contractors;
- approval of the design of security provisions for new plant or equipment.

2) *Security sensitive tasks*

This includes for instance the following:

- identification of security sensitive tasks;
- pre-determination and approval of secure working methods;
- pre-qualification of personnel for security sensitive tasks;
- procedures controlling the entry of personnel to security sensitive areas.

3) *Maintenance of security equipment*

This includes the following:

- segregation and control of access;
- inspection and testing of security related equipment and high integrity systems.

e) Typical outputs

Typical outputs include the following items:

- procedures;
- operating and maintenance instructions.

4.4.7 Emergency preparedness, response and security recovery

a) ISO 28000 requirement

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.

b) Intent

Preparedness, response and recovery following a security incident are covered by this section. The term emergency preparedness means plans, preparations and precautionary actions that are implemented following unplanned security events or crises.

The organization should actively assess potential incident and response needs for all potential security events identified through the threat identification and risk assessment process (see 4.3.1). Response plans, procedures and processes to cope with them, test planned responses and seek to improve the effectiveness of its responses should be developed.

c) Typical inputs

Typical inputs include the following items:

- security threat identification and risk assessment;
- availability of local emergency services and security agencies and details of any emergency response or consultation arrangements that have been agreed;
- regulatory, legal or other requirements;
- experiences and review of previous incidents and emergency situations and the results of subsequent actions;
- similar organizations' experiences from previous incidents and emergency situations (lessons learned, best practices);
- police, intelligence and first responders input;
- review of practice, exercises and drills performed.

d) Process

The organization should develop an emergency plan(s), identify and provide appropriate emergency arrangements and regularly test its capability through practice drills. Emergency preparedness, response and security recovery plans should include measures to restore security, protect data and facilities and assure security continuity.

Practice drills should test the effectiveness of the most critical parts of the security response plan(s) and the completeness of the emergency planning process. While desktop exercises can be useful during the planning process, realistic practice drills and exercises should be conducted. The results of emergencies and practice drills should be evaluated and changes that are identified as being necessary should be implemented.

1) *Emergency response and security recovery plan*

The emergency response and security recovery plan(s) should outline the actions to be taken when specified situations arise and should include the following:

- identification of potential incidents and emergencies;
- identification of the person to take charge during the emergency;
- details of actions to be taken by personnel during an emergency, including those actions to be taken by external personnel who are on the site of the emergency, such as contractors or visitors (who can be required, for example, to move to specified assembly of evacuation points);
- responsibility, authority and duties of personnel with specific roles during the emergency (e.g. security, fire-wardens, first-aid staff, radiological leak/toxic contamination specialists);
- evacuation procedures;
- procedures which describe how security measures and secure conditions are reinstated on the short and mid term;
- identification, location and protection of security materials, records, data and equipment and emergency action required;
- interface with emergency services and first responders;
- communication with stakeholders;
- availability of necessary information during the emergency e.g. plant layout drawings, security data, procedures, work instructions and contact telephone numbers;
- interface and communication with other supply chain business/trade partners;
- assure the integrity of communication systems.

The involvement of external agencies in emergency planning and response should be clearly documented. These agencies should be advised as to the possible circumstances of their involvement and provided with such information as they require facilitating their involvement in response activities.

2) *Security equipment*

Security equipment needs should be identified and equipment should be provided in adequate quantity. This should be tested at specified intervals for continuing operability.

3) *Practice drills and exercises*

Practice drills and exercises should be carried out according to a pre-determined schedule. Where appropriate and practicable, the participation of external security services in practice drills should be encouraged.

e) Typical outputs

Typical outputs include the following:

- documented emergency response and security recovery plans and procedures;
- security equipment list;
- test records for security equipment;
- practice drills and exercises;
- reviews of practice drills and exercises;
- recommended actions arising from the reviews;
- progress against the achievement of recommended actions;

- completed actions.

4.5 Checking and corrective action

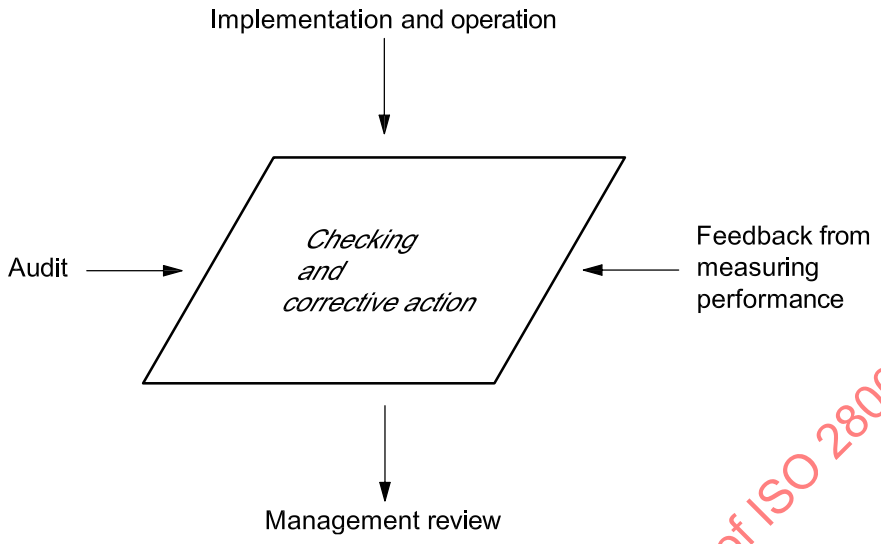

Figure 5 — Checking and corrective action

4.5.1 Security performance measurement and monitoring

a) ISO 28000 requirement

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 programmes, 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.

b) Intent

The organization should identify key performance indicators for its security performance across the whole organization and the supply chain that it either controls or has influence over. These should include, but not be limited to, measurable indicator that determine whether:

- the security policy and security objectives are being achieved;
- threats are being controlled and/or mitigated, as appropriate and countermeasures have been implemented and are effective;
- lessons are being learnt from security management system failures, including security incidents and near misses;
- awareness, training, communication and consultation programmes for employees and stakeholders are effective;
- information that can be used to review and improve aspects of the security management system is being produced and being used.

c) Typical inputs

Typical inputs include the following:

- security threat identification, risk assessment and risk management (see **4.3.1**);
- legislation requirements, regulations, best practices (if any);
- security policy and security objectives;
- procedure for dealing with non-conformances;
- security equipment test and calibration records (including those belonging to contractors);
- training records (including those belonging to contractors);
- management reports.

d) Process

1) *Proactive and reactive monitoring*

An organization's security management system should incorporate both proactive and reactive monitoring as follows:

- proactive monitoring should be used to check conformity to the organization's security activities, for example by monitoring the frequency and effectiveness of security inspections;
- reactive monitoring should be used to investigate, analyse and record security management system failures — including emergencies and security incidents.

Both proactive and reactive monitoring data are often used to determine whether security objectives are achieved.

2) *Measurement techniques*

The following are some examples of methods that can be used to measure security performance:

- results of security risk identification, risk assessment and risk control processes, such as compliance with WCO SAFE Framework of Standards and the United States' Customs - Trade Partnership Against Terrorism (C-TPAT) and European Commission Authorized Economic Operator (AEO) Regulation;
- systematic inspections using checklists;
- security inspections;
- evaluating new supply chain logistics systems;
- reviewing and evaluating resulting logistics statistical patterns;
- inspections of security equipment to check that they are in good condition;
- availability and effectiveness of use of personnel with recognized security experience or formal qualifications;
- behaviour sampling: assessing workers' behaviour to identifying poor security practices that might require correction;
- analysis of documentation and records;
- benchmarking against good security practices in other organizations;
- surveys to determine employee attitudes to detect suspect behaviour;
- Stakeholder feedback.

Organizations need to decide what to monitor and how often monitoring should take place based on the level of risk (see **4.3.1**). An inspection schedule based on security threat identification and risk assessment results, legislation and regulations should be prepared as part of the security management system.

Routine security monitoring of processes, logistic nodes, business partners, supply chain activities and practices should be carried out according to a documented monitoring scheme by authorised personnel, who should also undertake spot checks of critical tasks in order to assure conformity to security procedures and codes of practice. To assist in performing systematic inspections and monitoring, checklists can be used.

3) *Security equipment*

Security equipment that is used to monitor and assure security (e.g. cameras, fences, gates, alarms, etc.) should be listed, identified uniquely and controlled. The accuracy of this equipment should be known. Where necessary, written procedures should be available describing how security measurements are performed. Equipment used for security should be maintained in a proper manner and should be capable of performing as required.

When required, a calibration and maintenance scheme should be documented and implemented for the security equipment. This scheme should include the following items:

- the frequency of calibration and maintenance;
- reference to test methods, where applicable;
- identity of the equipment to be used for the calibration;
- action to be taken when the specified security equipment is found to be out of calibration.

Calibration and maintenance should be carried out under appropriate conditions. Procedures should be prepared for critical or difficult calibrations.

Equipment used for calibration should be in accordance with national standards where such standards exist. If no such standards exist, the basis for the levels used should be documented.

Records should be kept of all calibrations, maintenance activities and results. Records should give details of the measurements before and after adjustment.

The calibration status of security equipment should be clearly identified to the users.

Security equipment whose calibration or maintenance status is unknown or which is known to be out of calibration, should not be used. Additionally, it should be removed from use and be clearly labelled, tagged or otherwise marked, to prevent misuse. Such marking should be in accordance with written procedures. The procedures should include the identification of the calibration status of the product. A non-conformance should be issued to document the actions taken. The procedures should include an action plan if out-of-calibration equipment is discovered.

4) *Inspections*

i) *Equipment*

An inventory (using unique identification of all items) should be drawn up of all security equipment. Such equipment should be inspected as required and should be included in the inspection schemes.

ii) *Security inspections*

Security inspections should be carried out, but these should not absolve authorised personnel from carrying out regular inspections or from identifying security threats.

iii) *Inspection records*

A record should be kept of every security inspection carried out. The records should indicate whether or not documented security procedures were being conformed to. Records of security inspections, tours, surveys and security management system audits should be sampled to identify underlying causes of nonconformity and repetitive security risk. Any necessary preventive action should be taken. Security threatening situations and non conforming equipment identified during the inspections should be documented as non-conformances, assessed as to risk and corrected in accordance with the non-conformance procedure.

5) *Supplier (contractor) equipment*

Security equipment used by contractors should be subject to the same controls as in-house equipment. Contractors should be required to give assurances that their equipment conforms to these requirements. Prior to initiating the work, the supplier should provide a copy of its equipment test and maintenance records for any identified critical equipment that require such records. If any tasks require special training, the corresponding training records should be provided to the customer for review.

6) *Statistical or other theoretical analytical techniques*

Any statistical or other theoretical analytical technique used to assess a security situation, to investigate a security incident or failure or to assist in decision-making in relation to security should be based on sound

scientific principles. Top management should ensure that the need for such techniques is identified. Where appropriate, guidelines for their use should be documented, along with the circumstances in which they are appropriate.

e) Typical outputs

Typical outputs include the following items:

- procedure(s) for monitoring the effectiveness of security arrangements;
- inspection schedules and checklists;
- equipment inspection checklists;
- security equipment lists;
- calibration arrangements and calibration records;
- maintenance activities and results;
- completed checklists, inspection reports (security management system audit outputs, see **4.5.4**);
- non conformance reports;
- evidence of the results of implementing such procedure(s).

4.5.2 System evaluation

a) ISO 28000 requirement

The organization shall evaluate security management plans, procedures and capabilities through periodic reviews, testing, post-incident reports and 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.

b) Intent

Organizations should have effective procedures for reviewing and evaluating security management plans, procedures and their organisation's capabilities to meet their policy and objectives and targets. The organization shall also periodically review their compliance with applicable regulatory requirements.

The prime purpose of these procedures is to ensure that security plans and procedures are maintained up to date and in line with changing requirements and needs. These changes should be timely and take full account of any changes to the supply chain regulations, best practices and lessons learnt.

c) Typical inputs

Typical inputs should include:

- incident reports;
- results from incident planning and preparedness exercises;

- threat identification, risk assessment and risk control reports;
- security management system audit reports, including non conformance reports;
- incident and/or hazard reports;
- management review reports and actions (see 4.6);
- progress with achieving objectives;
- changing regulatory requirements;
- changing expectations of interested parties and stakeholders;
- changes to the organisations scope of work, activities and client base.

d) Process

The organization's management should at appropriate intervals conduct reviews of its security management system to establish and ensure its continuing suitability and effectiveness. The intervals should be sufficiently short so that failures of the systems can be identified before consequential damages arise.

The result of effective systems and their implementation, the achievement of objective and policy with be Continual Improvement, one of the unpinning principles of ISO 28000. The process and procedures required by clause 4.5.2 shall ensure that this is achieved.

e) Typical outputs

Typical outputs and results include:

- improved processes and performance;
- reduction of non conformance reports;
- legal compliance;
- updated threat identification, risk assessment reports and risk registers;
- improved processes;
- evidence of evaluations of the effectiveness of corrective and preventive actions taken.

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

a) ISO 28000 requirement

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:

   1) failures including near misses and false alarms;

   2) incidents and emergency situations;

   3) 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.

b) Intent

Organizations should have effective procedures for reporting and evaluating and/or investigating emergencies, security incidents and non-conformances. The prime purpose of the procedure(s) is to prevent further occurrence of the situation by identifying and dealing with the root cause(s). Furthermore, the procedures should enable the detection, analysis and elimination of potential causes of nonconformities including those resulting from human, system, process or equipment failures and errors.

c) Typical inputs

Typical inputs include the following items:

- procedures (in general);
- emergency plan;
- security threat identification, risk assessment and risk management;
- security management system audit reports, including non-conformance reports;
- security incidents and security threat reports;
- maintenance and service reports for security equipment.

d) Process

The organization is required to prepare documented procedures to ensure that security incidents and non-conformances are investigated and corrective and/or preventive actions initiated. Progress in the completion of corrective and preventive actions should be monitored and the effectiveness of such actions reviewed.

1) *Procedures*

The procedures should include consideration of the following items:

i) *General*

The procedure should:

- define the responsibilities and authority of the persons involved in implementing, reporting, investigating, follow-up and monitoring of corrective and preventive actions;
- require that all non-conformances, security incidents and security threats be reported;
- apply to all personnel (i.e. employees, temporary workers, contractor personnel, visitors and any other person involved in the supply chain);
- take into account impacts to stakeholders;
- ensure that no employee is criticized for reporting security incidents;
- clearly define the course of action to be taken following non-conformances identified in the security management system.

ii) *Immediate action*

Immediate action to correct the security incident should be taken when non-conformances, security incidents or threats are first identified. The procedures should:

- define the process for notification;
- where appropriate, include co-ordination with emergency plans and procedures;
- define the scale of investigative effort in relation to the potential or actual threat (e.g. include management in the investigation for serious security incidents).

iii) *Recording*

Appropriate means should be used to record the factual information and the results of the immediate investigation and the subsequent detailed investigation. The organization should ensure that the procedures are followed for:

- recording the details of the non-conformance, security incident or security threats;
- defining where the records are to be stored and responsibility for the storage.

iv) *Investigation*

The procedures should define how the investigation process should be handled. The procedures should identify:

- the type of events to be investigated (e.g. incidents that could have led to serious threat);

- the purpose of investigations;
- who is to investigate, the authority of the investigators, required qualifications (including line management when appropriate);
- the root cause of non-conformance;
- arrangements for witness interviews;
- practical issues such as availability of cameras and storage of evidence;
- investigation reporting arrangements including reporting to appropriate stakeholders.

Investigatory personnel should begin their preliminary analysis of the facts while further information is collected. Data collection and analysis should continue until an adequate and sufficiently comprehensive explanation is obtained.

v) *Corrective action*

Corrective actions are actions taken to identify the root cause(s) of non-conformances and security incidents and take steps in order to prevent recurrence. Examples of elements to be considered in establishing and maintaining corrective action procedures include:

- identification and implementation of corrective and preventive measures both for the short-term as well as long-term (this can also include the use of appropriate sources of information, such as advice from employees with security expertise);
- evaluation of any impact on security threat identification and risk assessment results [and any need to update security threat identification, risk assessment and risk management report(s)];
- recording any required changes in procedures resulting from the corrective action or security threat identification, risk assessment and management;
- application of risk management or modification of existing risk management, to ensure that corrective actions are taken and that they are effective.

vi) *Preventive action*

Preventive actions are actions taken to prevent potential security non conformances from occurring.

Examples of elements to be considered in establishing and maintaining preventive action procedures include:

- use of appropriate sources of information such as results of corrective actions, security incident trends, security management system audit reports, updated risk assessments, new information on security, advice from employees and stakeholders with security expertise, etc.;
- initiation and implementation of preventive action and the application of controls to ensure that it is effective;
- recording of any changes in procedures resulting from the preventive action and submission for approval.

vii) *Follow-up*

Corrective or preventive action taken should be as effective as practicable. Checks should be made on the effectiveness of corrective/preventive action taken. Outstanding/overdue actions should be reported to top management at the earliest opportunity.

2) *Non-conformance and security incident analysis*

Causes of non-conformances and security incidents should be categorized and analysed on a regular basis to enable a root cause analysis to be performed. Frequency and severity ratings should be bench marked with other supply chain stakeholders.

The following should be included in the categorization and analysis:

- reportable security incident frequency or severity rates;
- location, activity involved, agency involved, day, time of day (whichever is appropriate);
- type and degree or impact to facilities, supply chain, etc;
- direct and root causes.

Due attention should be given to security incidents. All security incidents could be an indicator of a security threat or vulnerability.

Valid conclusions should be drawn and corrective action taken. This analysis should be circulated to top management and included in the management review (see **4.6**).

3) *Monitoring and communicating results*

The effectiveness of security investigations and reporting should be assessed. The assessment should be objective and should yield a quantitative result where possible.

The organization, having learnt from the investigation, should:

- identify the root causes of deficiencies in the security management system and general management of the organization, where applicable;
- communicate findings and recommendations to management and relevant interested parties (see **4.4.3**);
- include relevant findings and recommendations from investigations in the continuing security review process;
- monitor the timely implementation of remedial controls and their subsequent effectiveness over time;
- apply the lessons learnt from the investigation of non conformances and security incidents across its whole organization, the supply chain it controls and has influence over, focusing on the broad principles involved, rather than being restricted to specific action designed to avoid repetition of a precisely similar event in the same area of the organization.

4) *Record keeping*

This can be accomplished rapidly and with a minimum of formal planning or it can be a more complex and long-term activity. The associated documentation should be appropriate to the level of corrective action.

Reports and suggestions should be sent to the top management's representative for analysis and retention (see 4.5.4).

The organization should maintain a record of security incidents. Such a records may be required by supply chain regulators.

e) Typical outputs

Typical outputs include the following items:

- security incident and non conformance procedure;
- non-conformance reports;
- non-conformance register;
- investigation reports;
- updated security risk identification, risk assessment and risk management reports;
- management review input;
- evidence of evaluations of the effectiveness of corrective and preventive actions taken.

4.5.4 Control of records

a) ISO 28000 requirement

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 personnel.

b) Intent

Records should be kept to demonstrate that the security management system operates effectively. Security records that support the management system and its conformance to the requirements should be prepared, maintained, be legible and adequately identified.

c) Typical inputs

Records (used to demonstrate conformance to the requirements) that should be kept include the following items:

- training and competence records;
- security inspection reports;
- security non conformances;
- results of preventive and corrective actions;
- security management system audit reports;
- security meeting minutes;
- reports of security exercises and drills;
- management reviews;
- security threat identification, risk assessment and risk management records.

d) Process

The requirement in ISO 28000 is largely self-explanatory. However, additional consideration should also be given to the following items:

- the authority for disposal of security records;
- confidentiality (protective marking) of security records;
- legal and other requirements on the retention of security records;
- issues surrounding the use of electronic records.

Security records should be fully filled out, legible and adequately identified. Retention times for security records should be defined. Records should be stored in a safe place, readily retrievable and protected from deterioration. Critical security records should be protected from possible fire and other damage as appropriate and as required by law.

e) Typical outputs

Typical outputs include the following items:

- procedure (for the identification, maintenance and disposition of security records);
- adequately stored and readily retrievable security records.

4.5.5 Audit

a) ISO 28000 requirement

The organization shall establish, implement and maintain a security management audit programme 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:

   1) conforms to planned arrangements for security management including the requirements of the whole of Clause 4 of this specification;

   2) has been properly implemented and maintained;

   3) 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 programme, 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.