BRITISH STANDARD

BS ISO 28004-1:2007

Incorporating corrigendum August 2012

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

ICS 03.100.10; 47.020.99

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Document Sharing Hub
British Standards

Full document details: BS ISO 28004-1:2007

National foreword

This British Standard is the UK implementation of ISO 28004-1:2007, incorporating corrigendum August 2012. It supersedes DD ISO/PAS 28004:2006 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee SME/32, Ships and marine technology - Steering committee.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2007

Amendments/corrigenda issued since publication

Date	Comments
30 April 2014	Implementation of ISO corrigendum August 2012: identifier updated throughout document from ISO 28004:2007 to ISO 28004-1:2007

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 81154 8

Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

INTERNATIONAL STANDARD

ISO 28004-1

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 28004-1:2007(E)

Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 2

3 Terms and definitions 2

4 Security management system elements 4
4.1 General requirements 4
4.2 Security management policy 5
4.3 Security risk assessment and planning 8
4.4 Implementation and operation 20
4.5 Checking and corrective action 34
4.6 Management review and continual improvement 49

Annex A (informative) **Correspondence between ISO 28000:2007, ISO 14001:2004 and ISO 9001:2000** 53

Bibliography 56

Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

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 28004-1 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 28004-1 cancels and replaces ISO/PAS 28004:2006, which has been technically revised.

Documents
Document Sharing Hub
Full document details: BS ISO 28004-1:2007

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.

Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

blank

Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

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.

Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

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.

Documents
Document Sharing Hub
Full document details: BS ISO 28004-1:2007

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

AVA Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

4 Security management system elements

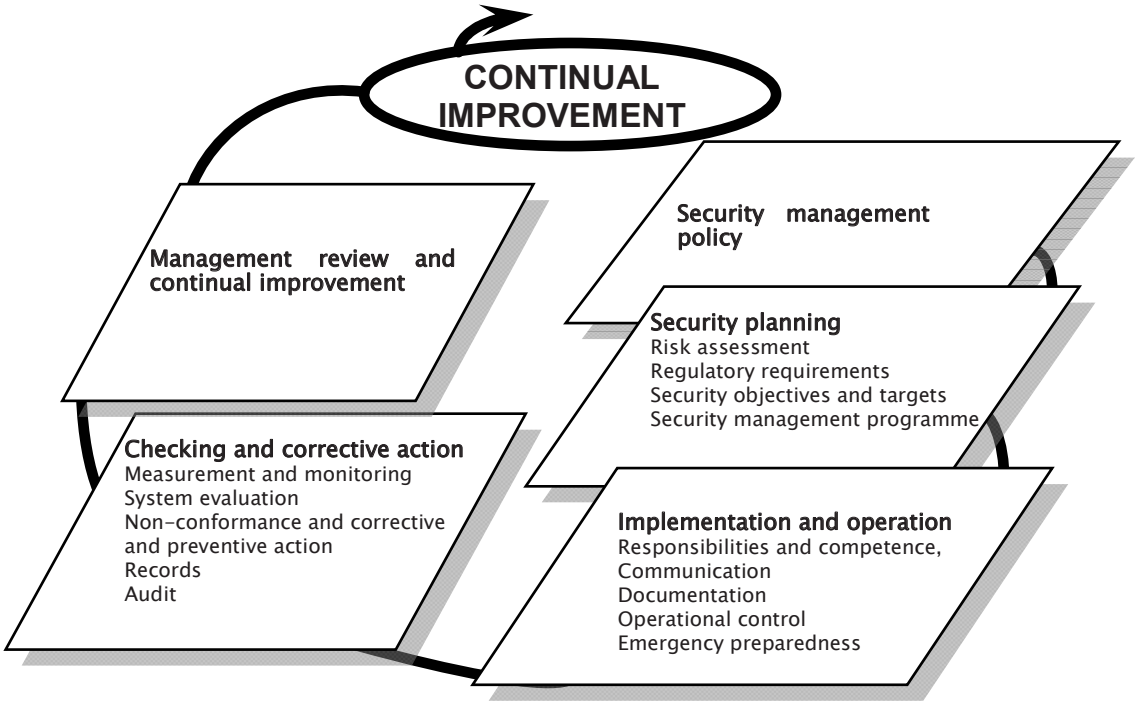

Figure 1 — Elements of successful security management

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.

Documents
Document Sharing Hub
Full document details: BS ISO 28004-1:2007

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

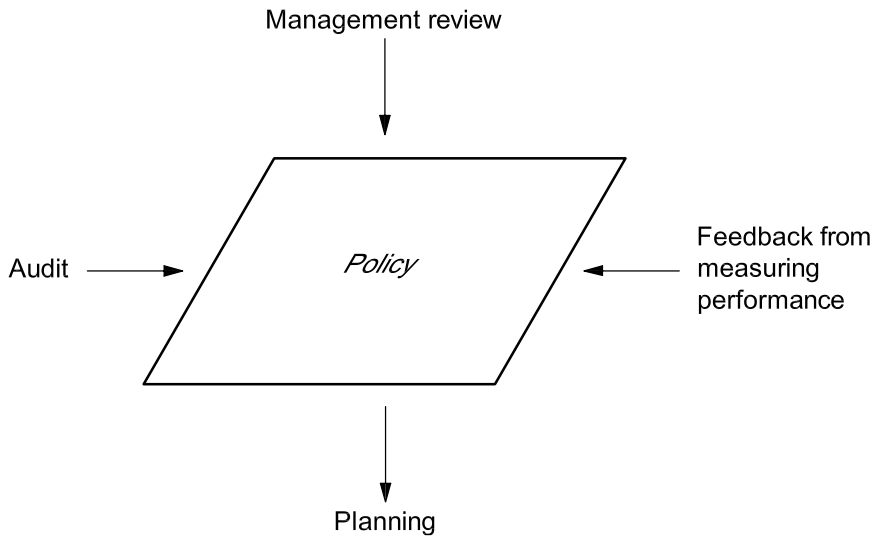

Figure 2 — Security management policy

Documents
Document Sharing Hub
Full document details: BS ISO 28004-1:2007

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;

Documents
Document Sharing Hub
Full document details: BS ISO 28004-1:2007

- 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;

AVA Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

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

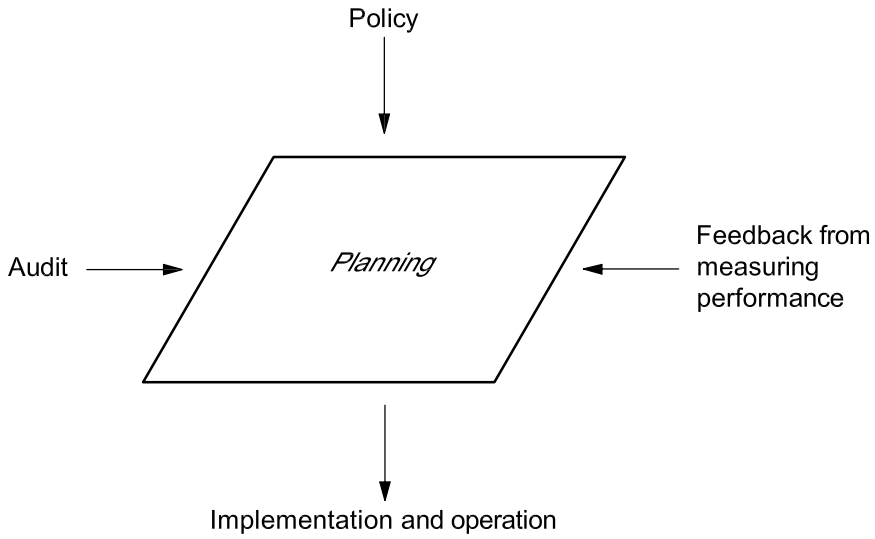

Figure 3 — Planning

Documents
Document Sharing Hub
Full document details: BS ISO 28004-1:2007

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).

Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

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**.

Documents
Document Sharing Hub
Full document details: BS ISO 28004-1:2007

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.

AVA Documents
Document Sharing Hub

Full document details: BS ISO 28004-1:2007

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;

Documents
Document Sharing Hub
Full document details: BS ISO 28004-1:2007