BS 16000:2015

BSI Standards Publication

Security management – Strategic and operational guidelines

bsi.

...making excellence a habit.™

Publishing and copyright information

Published by BSI Standards Limited 2015

ISBN 978 0 580 83490 5

ICS 03.100.01; 13.310

The following BSI references relate to the work on this document:
Committee reference SSM/1
Draft for comment 14/30285865 DC

Publication history

First published, June 2015

Amendments issued since publication

Date	Text affected

Contents

List of figures

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 22, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 30 June 2015. It was prepared by Technical Committee SSM/1, *Societal security management*. A list of organizations represented on this committee can be obtained on request to its secretary.

Use of this document

As a guide, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Contractual and legal considerations

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.

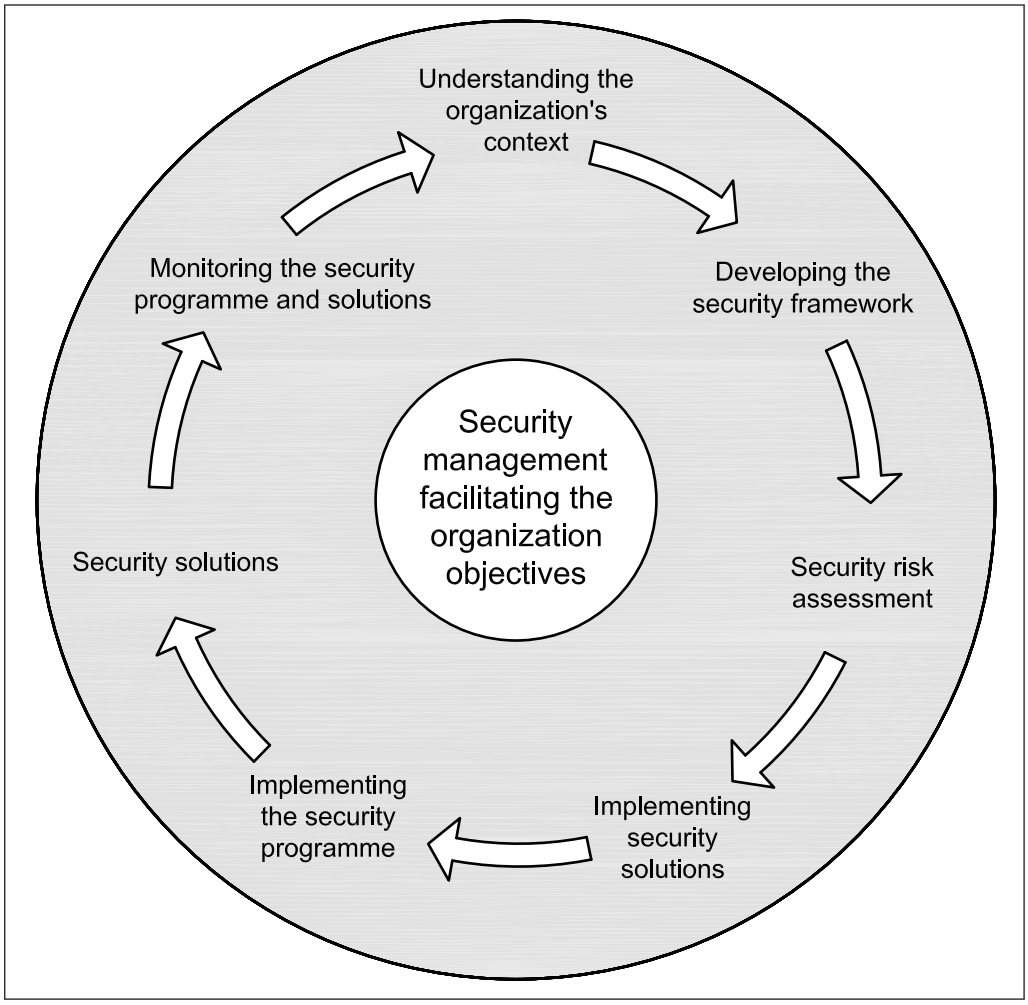
This page deliberately left blank

0 Introduction

Security management is a vitally important strategic capability for a modern organization that supports the achievement of the organization's objectives by protecting the organization's reputation and financial well-being. Indeed, beyond simply reacting to threats and risks, effective security management proactively supports both the capture and exploitation of opportunity and competitive or service delivery advantage.

As a management discipline, security management is best delivered when it follows a lifecycle process as shown in Figure 1.

Figure 1 **Embedding security management in the organization**



The application of the processes in Figure 1 to the various security domains might not all reside in any one area of the organization. Indeed, there are many different ways in which responsibilities can be split across a larger organization. Increasingly, good practice in security management acknowledges the need for close alignment between related security disciplines and, indeed, with other disciplines that rely upon, or are relied upon by, security, such as governance, resilience, risk management, business continuity and disaster recovery, asset management and crisis management. To achieve this, especially where convergence of these disciplines is not adopted as a corporate objective, a common understanding of the challenges in achieving security management is needed to ensure that all efforts are complementary.

Successful security is not done "to" the organization "by" a security function. It needs to be embedded in the organization's strategy and processes, such that security is done "by" the organization, which is supported by the security function. Everyone has a role to play in ensuring effective security within the organization.

Security management is one of the major responses to the risks identified by the organization. By definition, therefore, as every organization's risk appetite varies, it follows that the security management undertaken by the organization is bespoke. Security management does not necessarily involve either significant technology adoption and/or significant capital or revenue expenditure.

1 Scope

This British Standard gives guidance on security management for any organization, whether large or small, public or private, to support its viability, productivity, reputation, sustainability and, ultimately, success. The standard clarifies the basic principles of security management and demonstrates how security can be embedded in an organization.

An organization might already have implemented security solutions that have addressed some or all of its requirements, and this standard can be used to assist in the monitoring and review of the organization's security management and to determine how it might be improved.

2 Terms and definitions

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

2.1 countermeasure
action taken to counter or offset another action

2.2 governing body
individual or group of people ultimately responsible and accountable for the long-term direction and control of the organization

[SOURCE: BS 13500:2013, **2.8**]

2.3 likelihood
chance of something happening

NOTE 1 In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[SOURCE: PD ISO Guide 73:2009, **3.6.1.1**]

2.4 operational requirements
measures identified as necessary to address risks, threats and vulnerabilities

2.5 organizational resilience
ability of an organization to anticipate, prepare for, and respond and adapt to incremental change and sudden disruptions in order to survive and prosper

[SOURCE: BS 65000:2014, **2.3**]

NOTE Organizational resilience is a framework for bringing strategic direction and coherence to the full range of protective functions undertaken by an organization, including for example security management, risk management, business continuity management, supply chain management and crisis management.

2.6 residual risk
risk remaining after risk treatment

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as "retained risk".

[SOURCE: PD ISO Guide 73:2009, **3.8.1.6**]

2.7 risk
effect of uncertainty on objectives

NOTE 1 Although sometimes used colloquially to indicate something that is undesirable, "risk" as defined here is a neutral concept that is neither inherently desirable nor undesirable; willingness to accept some uncertainty (and therefore risk) is generally necessary in order to pursue objectives.

NOTE 2 Organizations typically have multiple objectives (such as those concerning financial, safety, environmental goals and reputation) which drive all aspects of the organization's activities (such as policies, strategies, projects, products and processes).

NOTE 3 Risk is often characterized by reference to the likelihood of experiencing consequences together with the potential for events from which such consequences could result.

NOTE 4 Uncertainty relates to a deficiency of information relevant to decision-making and takes many forms.

NOTE 5 See ISO/IEC Guide 51 for this term in the context of safety.

[SOURCE: PD ISO Guide 73:2009, **1.1**, modified]

2.8 risk acceptance
informed decision to take a particular risk

NOTE Risk acceptance can occur without risk treatment or during the process of risk treatment.

[SOURCE: PD ISO Guide 73:2009, **3.7.1.6**, modified]

2.9 risk analysis
process to comprehend the nature of risk and to determine the level of risk

NOTE 1 Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2 Risk analysis includes risk estimation.

NOTE 3 See ISO/IEC Guide 51 for this term in the context of safety.

[SOURCE: PD ISO Guide 73:2009, **3.6.1**]

2.10 risk appetite
amount and type of risk that an organization is willing to pursue or retain

[SOURCE: PD ISO Guide 73:2009, **3.7.1.2**]

2.11 risk assessment
overall process of risk identification, risk analysis and risk evaluation

NOTE See ISO/IEC Guide 51 for this term in the context of safety.

[SOURCE: PD ISO Guide 73:2009, **3.4.1**]

2.12 risk avoidance
informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk

NOTE Risk avoidance can be based on the result of risk evaluation and/or legal and regulatory obligations.

[SOURCE: PD ISO Guide 73:2009, **3.8.1.2**]

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

[SOURCE: PD ISO Guide 73:2009, **2.1**]

2.14 risk mitigation
measures taken to reduce an undesired consequence

2.15 risk sharing
form of risk treatment involving the agreed distribution of risk with other parties

NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate risk sharing.

NOTE 2 Risk sharing can be carried out through insurance or other forms of contract.

NOTE 3 The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

NOTE 4 Risk transfer is a form of risk sharing.

[SOURCE: PD ISO Guide 73:2009, **3.8.1.3**]

2.16 risk tolerance
organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives

NOTE Risk tolerance can be influenced by legal or regulatory requirements to ensure that no applicable law and no specific norm in the fields of safety, health or environmental protection is violated thereby.

[SOURCE: PD ISO Guide 73:2009, **3.7.1.3**, modified]

2.17 risk treatment
process to modify risk

NOTE 1 Risk treatment can involve:

- *avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;*
- *taking or increasing risk in order to pursue an opportunity provided no applicable law and no specific norm in the fields of safety, health or environmental protection is violated thereby;*
- *increasing risk in order to pursue an opportunity;*
- *removing the risk source;*
- *changing the likelihood;*

- *changing the consequences;*
- *sharing the risk with another party or parties (including contracts and risk financing); and*
- *retaining the risk by informed decision.*

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

NOTE 3 Risk treatment can create new risks or modify existing risks.

NOTE 4 See ISO/IEC Guide 51 for this term in the context of safety.

[SOURCE: PD ISO Guide 73:2009, **3.8.1**]

2.18 security
condition of being protected against damage, harm or loss, achieved through the management of adverse consequences associated with natural events and the intentional and/or unwanted actions of others by physical, technical, electronic, information technology (IT) or human factors, or a combination of those factors

2.19 security function
persons(s) responsible for managing security

2.20 security management
set of interrelated or interacting elements of an organization to establish security policies and objectives and processes to achieve those objectives

2.21 security management system
part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and progressively improves security management

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

2.22 security policy
corporate document setting out the organization's intentions and principles with regard to security, formally expressed by top management

2.23 security programme
outcome of the planning and implementation of the appropriate security measures, encompassing everything that is happening or needs to happen in terms of ensuring the security of the organization

2.24 standard security procedure (SSP)
written instructions to achieve uniformity of performance of a specific function(s)

NOTE These may be called "standard operating procedures" (SOPs) and "assignment instructions" (AIs).

2.25 threat
action or potential action likely to cause damage, harm or loss

EXAMPLES

physical; biological; chemical; ergonomic; psychological; criminal; fire, environmental, natural disaster; civil disturbance; espionage.

2.26 top management
person or group of people who controls the management functions of an organization on a day-to-day basis

NOTE Top management has the power to delegate authority and provide resources within the organization.

[SOURCE: ISO/IEC Annex SL:2012, **3.05**, modified]

2.27 vulnerability
intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence

[SOURCE: PD ISO Guide 73:2009, **3.6.1.6**]

3 Understanding the organization's context

3.1 General

Security management is not an end in itself; rather, it is a means to an end. Consequently, effective security, as a strategically valuable capability, should principally and initially understand the context in which the organization operates, the way in which the capability is to be developed, and how the organization can subsequently exploit it.

It is therefore almost always inappropriate for those building an understanding of the organization's context to assume that they are "starting from scratch". Related disciplines (see 0 Introduction) are likely to have considered the context in essentially the same way, especially if they are operated as a management system. The information held by those undertaking these activities is highly relevant to effective security management. As a result, the task here is essentially one of extrapolation, extension or conversion of that knowledge to support security management.

3.2 External context

Increasingly, organizations are obliged to meet external expectations in respect of security. Whilst these can take the form of legal and regulatory obligations, they are often much wider than this.

Considering external stakeholders (shareholders, community groups, pressure and protest groups, politicians, the public, etc.) enables the organization to address a variety of factors relevant to success, not least public perception and the reputation of the organization, for which security management is a key enabler.

It is neither appropriate nor possible to be definitive about all the external factors to consider, but as wide a review as possible should be attempted. Clearly, the level of crime present in the locations in which the organization operates is important. To ensure that all relevant external factors are considered, those addressing security management should make a particular point of engaging with the organization's strategy function wherever such a function exists.

3.3 Internal context

3.3.1 General

It is likely that an extensive range of activities is undertaken by the organization, many of which have a reliance upon security management and a different subset of which are already contributing indirectly to security management.

3.3.2 Objectives and strategy

If security management is about enabling the success of the organization, the fundamental internal context required is the objectives of the organization and an understanding of the strategy being pursued to deliver those objectives. These should be used to define the required scope of security management and its contribution to building organizational resilience (see BS 65000). They may also be used to discuss and agree at least an initial version of the security management framework required to facilitate the attainment of the objectives (further discussed in Clause **4**).

3.3.3 Major risks and risk appetite

It is important to understand the extent to which the process of setting the objectives considered the risks to them and of them and, as a result, the degree of risk that the organization is prepared to tolerate.

Furthermore, security as a strategic enabler should be primarily focused on addressing major risks. Whilst any security management function is likely to identify additional major risks, the principal benefit of security management is its positive impact on the organization's perceived major risks.

This also facilitates a dialogue with the members of the governing body. It might be that not all the risks have been captured; the recording could be informal or non-existent; and the risk assessment might have overlooked key factors. Nonetheless, the security management function, even if "in waiting", can therefore have both a particularly positive early impact and justify itself further.

This is a particularly important input to the identification of the full spectrum of security risks that the organization has to assess and treat appropriately and commensurately.

3.3.4 Organization structures and accountabilities

The organization should compile a coherent profile of the organization's structure, processes, people, activities, and the locations and other environments in which it operates. A strong understanding of the organization's supply chains should also be captured.

Particular attention should be given to identifying the functions that already have (explicit or implicit) "security" responsibilities within their scope or which deliver closely related activities.

In the process of this activity it should be possible to clarify the governing body's accountability (see BS 13500) for security management.

3.3.5 Leadership, awareness and culture

The organization should consider how well the governing body (see BS 13500) and top management (where different) provide leadership, i.e. the extent to which they "practise what they preach" and "play to the same rules". This is often closely coupled to the level of awareness that the organization has of security. Clearly, the organization's partners, staff and management cannot be expected to exhibit the right behaviours and culture if they are unaware of the concepts.

Understanding this position allows early, interim activity to address any deficiencies, the delivery of which (as part of the framework described in Clause **4**) will have fundamental, significant and early benefits to the organization.

3.3.6 Stakeholders' expectations

The final step toward understanding the internal context should be to revisit the expectations of stakeholders. Organizations increasingly recognize the needs and security risks emanating from the needs of their staff, partners, suppliers, service providers and others. The security of an organization is often in the hands of, and might even delivered by, others. Security management should therefore understand and document these such that sufficient "end-to-end" security can ultimately be delivered.

3.4 Deriving requirements for security management

The understanding gained in **3.1** to **3.3** should be used to define a set of high-level objectives against which the (future) security management function (if required) can be continuously evaluated. This is described further in Clause **9**.

In addition to the objectives, the organization should identify critical success factors (CSFs) for security management. Both should be inputs into the risk assessment to deliver key performance indicators (KPIs) and metrics to establish whether the objectives and CSFs are being met. This is discussed further in Clause **9**.

4 Developing the security framework

4.1 General

The understanding of the organization's context and objectives should be used to commence the development of the management and operational framework for security. However, as the risks have not yet been fully assessed and appropriate controls selected and implemented, the framework cannot be fully developed. Nonetheless, even the act of defining and deploying this interim framework with some associated improvement actions will begin to reduce the security and other risks.

Furthermore, developing the initial security framework itself directly enables the execution of the security management activities defined in Clause **5** to Clause **9**.

4.2 Commitment to security management

The organization should document its context and objectives in a security management statement of intent and make this very visible to all the stakeholders with which it interacts. At the very least, this document should act as a "holding measure" pending the creation of a fuller security management policy described in **7.2**.

4.3 Communication and awareness

It is a fundamental principle of security management that the organization's workforce, its stakeholders and suppliers and partners all have a pivotal role in maintaining effective security, i.e. security is everyone's business, rather than the preserve of a security management function.

However, individuals cannot be expected to change their behaviours, and thereby contribute to the enhancement of the organization's security culture, without raising awareness.

Therefore, the organization's governing body and top management should consider how to communicate the statement of intent and commitment as their first communication to their stakeholders.

4.4 Organization structure and roles and responsibilities

The organization should establish a security management structure, with an appropriate working group at its core. The organization should seek to build in efficiency and effectiveness by looking for opportunities to augment an existing group wherever possible, rather than create an additional group. This security management group, with appropriate terms of reference and membership to ensure full organizational representation, should be directly and clearly linked into the organization's governance structure.

It is also probable that the organization will need to allocate new and additional roles and responsibilities to individuals. This should be done formally, clearly and in writing, and should flow through into individuals' objectives and performance rewards.

These roles and responsibilities should include the following.

a) Governing body

- Retaining overall accountability for security management.
- Identifying a specific member of top management with accountability for security.
- Providing clear direction to the member of top management.
- Demonstrating commitment to security management.
- Obtaining, and acting upon, evidence of the effectiveness or otherwise of security management.

b) Top management

- Ultimate accountability for the development and implementation of the security management framework and associated organization structure, as well as a security improvement programme to fully meet the agreed objectives, manage the security risks and contribute to the management of other risks to those objectives.
- Appointing a sufficiently dedicated and appropriately competent person to be responsible day-to-day for security, who has access to top management.
- Promoting security cultural change throughout the organization, by way of security awareness and appropriate security training for staff.
- Liaison with security, policing, regulatory and other agencies that either have responsibilities for delivering or facilitating security or an interest in sharing in the lessons from it.
- Active engagement, and mutual support, with peers who hold responsibility for both elements of security management and functions that support it.
- Coordination and facilitation of whatever security management group is established.
- Ongoing management of the human and other resources allocated to achieve appropriate security management.
- Ensuring the creation, operation and continuous improvement of the security management framework and lifecycle processes.
- Reporting to the identified governing body holding accountability for security management on all matters related to the effectiveness and efficiency of security management.

c) Staff

- Applying and remaining in compliance with policies and procedures in which they have been trained or made aware.

- Following security escalation processes for reporting of suspicious incidents/items, including near misses, and "whistleblowing" when this appears justified.
- Communicating information on threats, impacts and risks wherever and whenever they observe or suspect these.

4.5 Security advice

The selection, implementation and operation of the correct security solutions can be a daunting task for non-security decision-makers, as the security solutions available are numerous and their suitability is related to the organization's risks and risk tolerance and what can be afforded, which is dependent upon budget availability.

Security advice is available from a number of sources, including:

a) local police crime prevention officers (who can also supply local crime information);

b) security professionals and practitioners with the necessary competences, as demonstrated by academic and/or chartered qualifications, membership of professional institutes/associations, or relevant experience and testimonials;

c) security solutions providers; and

d) the Centre for the Protection of National Infrastructure (CPNI).

5 Security risk assessment

5.1 General

Developing a security plan requires a security risk assessment to be conducted to identify the organization's assets, the threats to the assets and the likelihood of each threat becoming a reality.

5.2 Asset identification

It is important to identify which assets require protection, and how much, their importance to the organization and how they are interdependent. An asset is something of value to the organization that requires protection. Assets are varied and include people, property, buildings, information, processes and reputation. These can be tangible assets (e.g. equipment) or intangible (e.g. reputation and intellectual property).

Different assets require different levels of security and protection, and identifying them enables appropriate levels of protection to be planned, e.g. a laptop might easily be replaced, but the files and data it contains might be irreplaceable or of value to a competitor. For example, failure in a supply chain can impact on the value of the organization's assets, so this needs to be considered when assessing the nature of the assets.

5.3 Security threat and risk analysis

It is vital for the organization to understand the threats and vulnerabilities it faces in order to determine the nature of the security programme and control measures. Having conducted the risk analysis, therefore, the organization should evaluate the specific likelihood and impact of those threats and vulnerabilities which affect and/or impact the organization and its assets.

NOTE See BS ISO 31000 and BS 31100.

A threat is a source of potential harm to an identified asset which might cause damage, loss or injury. Threats are varied and include:

a) terrorism;

b) opportunist crime, e.g. theft of unattended laptops and bicycles;

c) hostile acts by insiders;

d) organized crime, e.g. robbery, fraud, counterfeiting and diversion;

e) cybercrime and data breaches;

f) single-issue/political extremism, e.g. animal rights activists, environmental extremists and anti-capitalist protests;

g) socio-economic issues, e.g. antisocial behaviour and street riots; and

h) environmental/natural/incident/crisis, e.g. floods, fire, drought and rail crashes.

The vulnerability of an asset depends on where it is located, who has access to it, its attractiveness to a threat adversary, and the effectiveness of the controls in place.

The advice of external agencies, e.g. the police, and neighbours should be sought to help identify and assess the threats and levels of threats. There are also other sources of published information, e.g. websites showing internet connection or whether the area is in a flood plain.

Some organizations are more vulnerable to certain kinds of threats by virtue of the nature of their activities, ownership, location, reputation and other factors, e.g. a business operating in a high-risk environment, such as a theatre of war or area of social unrest, or a business creating high-value property. Nonetheless, small businesses operating in areas with high levels of petty crime could be at risk.

5.4 Risk register

The security risk and threat assessment can, if considered helpful, be documented using a risk register showing:

a) a description of each risk or threat;

b) the likelihood of the security risk/threat taking place;

c) the consequence to the organization if the security risk/threat is realized;

d) the importance of the security risk/threat to the organization;

e) how current controls manage the security risk/threat; and

f) performance against expected outcomes.

Risk registers can support the visibility of agreed risk and facilitate their periodic review.

6 Implementing security solutions

6.1 General

An analysis of existing security measures is useful in identifying the steps necessary to enhance the security of the organization. It also consists of a review of the security measures required for a new site/location, whether locally or internationally. From this, an evaluation can be made of the potential credible consequence and impact if an event were to occur.

The risks identified during the analysis should be ranked in order of priority, so that appropriate, proportionate mitigation measures can be applied to manage any risk consistent with the organization's risk appetite. The organization should identify the options available for addressing each risk, taking account of existing controls, the outcomes of which may include:

a) avoidance;

b) transfer/sharing;

c) elimination;

d) mitigation;

e) tolerance/acceptance.

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits expected.

Prior to procuring security products and/or services, the organization's operational requirements should be fully defined and recorded following the process in Clause **3** to **6.6**.

NOTE The CPNI gives further information on producing operational requirements for security measures [1].

Any control measures proposed to achieve these outcomes should be proportionate to the security risk(s) posed and provide a positive return on security investment.

6.2 Avoidance

Where risks cannot be influenced by the organization and/or cannot be managed to an acceptable level, the only option might be to not proceed with an activity or to withdraw from it. An example is where an area intended for new premises is identified as having a high crime rate.

6.3 Transfer/sharing

For some risks the most appropriate response might be to transfer them (often referred to as "risk sharing"). An example is where a small tenant in a much larger premises owned or leased by another organization transfers responsibility for closed-circuit television (CCTV) coverage to the other organization. The organization transferring the risk, though, acquires a new risk that the organization to which the risk is transferred might not manage the risk effectively.

6.4 Elimination

The decision might be taken to eliminate certain risks, e.g. the risk of tailgating (an unauthorized person following an authorized person through an entry point to the premises) might be eliminated by installing airlocks or turnstiles.

6.5 Mitigation

Mitigation involves reducing the impact of certain risks, e.g. implementing search procedures can mitigate the risk of staff or visitors entering the building with weapons, an adequate response and effective recovery.

6.6 Tolerance/acceptance

Tolerance/acceptance involves planning no further action to respond to residual risk for the time being. A risk might be retained because no further worthwhile actions can be devised, or because the only remaining responses are unacceptable for some reason or cannot yet be implemented. Risk retention has to be a conscious decision, signed off by top management, based on the results of the risk analysis and evaluation process, but might need to be reviewed when circumstances change.

7 Implementing the security programme

7.1 Programme management and accountability

Having identified and selected from the options available for addressing the risks referred to in Clause **6**, an appropriately skilled individual should be made responsible for overseeing the implementation of the appropriate solutions, including the controls and countermeasures.

However, the accountability for the effectiveness of the programme remains with the governing body and top management, who should publicly endorse and support the programme's execution.

7.2 Security policies

Security policies should be prepared for all appropriate types of assets, e.g. information, physical aspects, IT and personnel. The security policies may comprise:

a) a mission statement;

b) a general policy statement;

c) management strategies and allocation of security responsibilities and resources;

d) standard security procedures; and

e) audit and compliance.

Appropriate security policies set the direction for the implementation of the security strategy and programme to deliver the expectations of top management and stakeholders.

7.3 Security programme

7.3.1 Planning the security programme

Planning the security programme sets out the proportionate steps to reduce identified risks to a level that is as low as reasonably practicable, based upon a formal security risk analysis (see Clause **5**).

This is communicated throughout the organization in a variety of formats, usually as security standards or guidance/guidelines.

Development of the security programme is managed by those nominated (see Clause **5**) and other (internal and external) stakeholders, e.g. finance, commercial and IT.

7.3.2 Implementation of the security programme

In accordance with the defined security policy, every security programme requires appropriate security procedures in order to achieve optimum and safe results. Examples of subject matter include: roles and responsibilities, management and operation of physical and electronic security/management systems (e.g. CCTV, document control, intruder alarms, access control, searching), training, and risk, incident and crisis management (see BS 11200). Even the most enthusiastic security team, operating alongside the most advanced technology, might not succeed without the support of clearly defined, and easy to understand, operating procedures.

8 Security solutions

8.1 General

The security function should oversee the operational, physical, procedural, technical and personnel solutions of the security strategy.
Subclauses **8.2** to **8.9** set out non-exhaustive lists of solutions that can be drawn upon to deliver an effective security programme for the organization.

The operational requirements should reflect the security policy and programme (see Clause **7**). The security function needs to consider all of the following points to identify what is relevant to the organization and to the specific security programme:

a) preparing a statement of the operational requirements, taking account of budgetary and resource constraints, such as equipment/security management systems (e.g. CCTV, access control and lighting);

b) standard procedures; additional security measurements for the security of high-value assets, physical or intangible, the loss of, or damage to, which would cause negative impact on the organization;

c) maintaining and evidencing compliance with all appropriate legislation, regulations and policies;

d) ensuring that the physical equipment is provided, and procedures and other technical measures are implemented;

e) ensuring appropriate reporting processes and data are in place; and

f) ongoing management, supervision and monitoring of the security programme.

NOTE The CPNI gives further information on producing operational requirements for security measures [1].

The security function should, by applying a structured, evidence-based methodology, identify appropriate physical, technical and related solutions necessary to ensure the security of the organization, its people, premises and other assets. These should ensure:

1) an effective deterrence, detection and apprehension capability;

2) conditions are made more difficult for an offence/adverse act to occur; and

3) the time it takes to commit an offence/adverse act is extended, thereby increasing the possibility of detection and response.

The application of the appropriate physical, technical, IT and/or manned solution achieves a higher security if the security solution takes into account "in-depth protection". This acts to present consecutive security barriers to a wrongdoer. The barriers can be physical, technological or security guarding, or a combination of these.

8.2 Physical security

Physical security should take into account the control of access (access control), e.g. the building's entry and exit points (including fire escapes) which restrict the flow of people into and out of the organization's building(s).

Physical security puts a physical barrier in the way of a wrongdoer to deter them from achieving their aim. Examples include:

a) perimeter security: fences, gates, bollards, barriers, etc.;

b) building security: security of doors and windows, airlocks, rising screens and shutters, etc.; and

c) point security: safes, secure cabinets, physical locks on computers, etc.

NOTE Physical security also includes features such as ditches, hedges and plants which act as a natural deterrent.

8.3 Technical security

The application of technology can support the physical security by deterring and detecting wrongdoers. Technical security includes, for example:

a) perimeter security: perimeter intruder detection systems (PIDS), CCTV systems (including number plate recognition systems and video analytics), barrier access control systems, intercom systems, security lighting, etc.;

b) building security: access control systems (barriers against unauthorized entry/removal of assets), biometrics, intruder alarms systems, CCTV systems, etc.;

c) point security: radio frequency identification (RFID), biometric locks on computers, etc.; and

d) design, e.g. architectural design and use of colour to deter or encourage behaviours (red boundaries and green paths, etc.).

Technical security can involve the remote monitoring of the organization's sites by third-party security monitoring centres which respond to the activations/ alarms received and ensure that the most appropriate (emergency) response is summoned. The type of response is agreed between the organization and their security provider.

Communications should also be taken into account to ensure that all security operatives within the organization and any contact with any external organizations (police, fire brigade) or contracted security providers [key holding response (see **8.4**)] is set down and contacted procedures agreed. This should also include communications in case of emergencies.

8.4 Manned security

Manned security provides security officers to deter, detect and apprehend wrongdoers. Security officers can provide a number of security functions for an organization, such as:

a) concierge duties;

b) 24-hour on-site protection;

c) patrolling duties (both foot patrol and mobile patrol);

d) key holding response (response to technical systems alarms);

e) manning gate posts for vehicle and personnel entry/exit points;

f) operation of security systems (including onsite CCTV); and

g) carry out security screening (x-ray machines, explosive detection, drug detection, etc.).

NOTE In the UK, contracted manned guarding as defined by The Private Security Industry Act 2001 [2] is required by law to carry a government licence to work (see http://www.sia.homeoffice.gov.uk/Pages/home.aspx) [viewed 2015-06-29].

8.5 Information security

The protection of information (data) is fundamental to the well-being of any organization. Information security should be built into the business process and be an integral part of the security programme (see also BS ISO/IEC 27001). Protecting the confidentiality, integrity and availability of information protects the organization and its reputation.

The organization should identify the relevant risks, threats and vulnerabilities in the way that information technology is used to support the organization's activities and should consider the full range of issues, for example:

a) authenticating all staff with access to information, including customers and contractors;

b) developing a communications policy that clearly outlines how staff are to use communication systems (computers and portable devices) in or out of the organization (i.e. on business trips or home working), including restrictions on the use of portable media devices (with appropriate encryption) to download information or to upload information, and details of how staff are to use the internet, emails and remote access to IT resources;

c) controlling staff access to information and limiting information on a "need-to-know" basis by creating and enforcing an information access hierarchy;

d) protecting IT equipment using physical security to reduce/restrict access to where the information can be obtained or stored, with support from technical and manned security;

e) maintaining up-to-date operating systems on servers and personnel devices used for business, as well as software run on these;

f) putting logical controls (e.g. computer passwords, firewalls, data encryption, network intrusion detection systems, security software) in place to protect information and ensuring that these controls are updated/changed regularly;

g) securely destroying obsolete information (by, for example, shredding) and wiping or physically destroying IT equipment before it is disposed of;

h) implementing appropriate and proportionate identity and access management controls with periodic reviews of usage, entitlements and applicability; and

i) specific issues relating to the organization's usage of "cloud" based services and other relevant services provided by third party suppliers and vendors.

8.6 Procedural security

For the avoidance of doubt, security procedures [sometimes referred to as "standard operating procedures" (SOPs)], should be clearly defined and workable, and communicated to (and understood and accepted by) appropriate management and staff/other personnel. Complicated procedures are typically unhelpful and confusing when personnel are likely to be operating under pressure.

8.7 Asset management

The organization should identify and manage its assets to collect the right information and put systems in place for effective asset management. Asset management is a key element in keeping assets safe and secure, and to prevent them from being lost, stolen or damaged. Assets include:

a) keys;

b) stock, i.e. classes of goods;

c) IT equipment, i.e. laptops, mobile phones, cables;

d) vehicles;

e) cash;

f) commercial;

g) fixtures and fittings; and

h) people, including lone workers.

The organization should have an adequate management information system or register to track or log the actual life of individual assets, ensuring it is kept up to date and reviewed on a regular basis.

Depending on the nature of each asset, it is likely to be used in a variety of different ways and settings. For example, it may be used by a subcontractor or a member of staff within a particular department. In some cases it might be shared across departments/divisions. Where possible, identification of staff and contractors using security passes or badges should be part of an overall security solution that is monitored and reviewed as part of the overall security standards as outlined in the security policy.

Types of systems for managing assets and people, i.e. visitors and subcontractors, include:

1) CCTV – monitoring;

2) access control;

3) integrated security systems;

4) key management and control;

5) locks;

6) security marking and asset tagging; and

7) counterfeiting control (see BS ISO 12931).

The organization should take into account other work activities outside the premises in the way assets are used and managed. For example, monitoring assets and people that might not be on site all the time (e.g. home workers, delivery drivers) should be protected from vulnerabilities and compromises from unauthorized users.

The organization should take into account the ownership of the assets used on its behalf and what responsibilities it has for the protection of assets owned by third parties, e.g. hired vehicles, plant and equipment.

NOTE Further information is given in BS ISO 55000.

8.8 Personnel security

8.8.1 Personnel selection

Perhaps the greatest security threat, or potentially damaging threat, to an organization is from employees or people with access inside the organization to its critical assets or information, e.g. theft, fraud and malice.

To manage this threat, the organization should sustain a through-life approach to monitoring the performance of, and degree of trust that can be invested in, its personnel. This should begin with pre-employment screening to confirm the accuracy of information provided by an applicant.

NOTE A process for pre-employment screening that has been widely recognized as good practice by many organizations and sectors is given in BS 7858.

The organization should then be able to match the suitability of different personnel with the sensitivity of the organization's activities. In particular, when personnel are required to change roles or take on additional responsibilities, the organization should actively consider rescreening these individuals.

The organization should establish a policy and escalation process for the resolution of any anomalies identified in the security vetting process, using a risk-based approach. Such a process should be fully documented and the organization should determine an appropriate and proportional document retention period for the material generated during the vetting stage.

The organization should also determine the level of any vetting and background checks to be performed on any subcontractors or temporary staff who might have access to the organizations critical assets or information.

The organization should consider whether or not the vetting process is to be repeated at appropriate time intervals during the employment period of any particular individuals. Any decision by the organization on repetition of vetting and frequency should be based on risk, and should be appropriate and proportional to the risk landscape and any relevant cost-benefit analysis.

8.8.2 Training and development

An appropriate training and development programme should be implemented for all individuals, aligned to their particular roles and responsibilities.

8.9 Security in procurement

There are different elements to the procurement process when delivering security, which include security of the procurement processes, procuring security solutions that conform to the processes and policies of the organization, and inclusion of security requirements in other procurements.

NOTE The CPNI provides further information on producing operational requirements for security measures [1].

9 Monitoring the security programme and solutions

9.1 General

The organization should ensure that it regularly reviews its requirements for security and monitors the operation of the security management arrangements that it has implemented.

These reviews should take the form of structured audits using a combination of operational managers, other internal resources not directly involved in security management and, if considered justified by the risks being managed, resources from third parties.

9.2 Security monitoring and reporting

The security management system should receive regular reporting of security monitoring activities and outcomes. Additionally, the organization's operational managers should be required to report on their security management responsibilities as part of their standard reporting. This should include the status of all risks that have been accepted.

9.3 Regular reassessment of risks

The risk landscape is variable and constantly evolves. The organization's risk profile should therefore be reviewed regularly (see Clause **5**). This review should consider what new risks have emerged, which existing risks have increased and which reduced. The review should also consider what risks are no longer tolerable and the extent to which the organization's risk appetite and capability to tolerate risks has increased, such that the opportunity might exist to remove controls that have already been implemented.

9.4 Reviewing the security framework

As well as reviewing the efficacy of the controls managed within the framework, the organization should periodically review the effectiveness of the security framework itself (see Clause **4**). Consideration should be given to the accountability for security management, the clarity, completeness and awareness of roles and responsibilities, and role holders' individual effectiveness.

9.5 Exercising and testing

Circumstances change, so systems and plans should be tested and drilled frequently, according to such factors as the size and scale of the organization.

The object of tests and drills should be to determine whether the processes and system implemented satisfy the policy and programme that have been defined. A security system or plan (e.g. security, crisis and continuity) that has never been tested and drilled might not work when needed.

People learn best by "doing", so regular testing can be carried out through:

a) an orientation or "walk through";

b) a table-top exercise;

c) a functional test, such as an evacuation; and

d) a full-scale test to evaluate the responses across the organization, its suppliers and partners.

9.6 Auditing

Premises, threat levels and circumstances are all likely to change over time, so the security system should be kept constantly under review.

To ensure and maintain the effectiveness of the current security policy the organization should create an audit policy, under which audits are conducted at regular, specified intervals, and the results and actions documented. The objective of an audit is to determine whether the current policy and programme are still adequate to address all currently assessed risks and threats.

It might also be advisable to periodically use the professional expertise of external security specialists or auditors.

This regular audit history provides a record of activities demonstrating the organization's commitment and actions to maintain and adhere to the security policy.

9.7 Management consideration of monitoring and review results

The monitoring and review findings should be documented and further considered as part of a specific item in the organization's routine management meetings, when changes to the organization's context (see Clause **3**) should also be considered.

If a deficiency is identified in the security programme, consideration should be given as to whether to update the security policy or programme or enhance the internal monitoring process.

The conclusions of the management review meetings should be communicated to all the appropriate personnel of the organization, to ensure that they are aware of any new requirements and the reasons for them, and to demonstrate both the governing body's expectations and execution of their accountability for security management.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 7858, *Security screening of individuals employed in a security environment – Code of practice*

BS 11200, *Crisis management – Guidance and good practice*

BS 13500:2013, *Code of practice for delivering effective governance of organizations*

BS 31100, *Risk management – Code of practice and guidance for the implementation of BS ISO 31000*

BS 65000:2014, *Guidance on organizational resilience*

BS ISO 12931, *Performance criteria for authentication solutions used to combat counterfeiting of material goods*

BS ISO 31000, *Risk management – Principles and guidelines*

BS ISO 55000, *Asset management – Overview, principles and terminology*

BS ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC Annex SL:2012, *Proposals for management system standards*

ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

PD ISO Guide 73:2009, *Risk management – Vocabulary*

Other publications

[1] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE (CPNI). *Guide to Producing Operational Requirements for Security Measures*. CPNI. 2013 (http://www.cpni.gov.uk/documents/publications/2010/2010001-op_reqs.pdf) [viewed 2015-06-29]

[2] GREAT BRITAIN. The Private Security Industry Act 2001. London: TSO.

Further reading

There is a growing wealth of literature relevant to security management, much of which has influenced the development of this guide. Some of this literature is included here, with the caveat that the list is limited and is not, and cannot be, in any way definitive or exhaustive.

ANSI/ASIS PAP.1:2012, *Security Management Standard: Physical Asset Protection.*

ASSOCIATION OF CHIEF POLICE OFFICERS IN ENGLAND, WALES AND NORTHERN IRELAND (ACPO) [1]. *Security Systems Policy*. London: ACPO. 2014.

BS 7499, *Static site guarding and mobile patrol service – Code of practice.*

BS 10501, *Guide to implementing procurement fraud controls.*

BS EN 31010, *Risk management – Risk assessment techniques.*

BS EN ISO 22313, *Societal security – Business continuity management systems – Guidance.*

BS ISO 22301, *Societal security – Business continuity management systems – Requirements*

[1] Now National Police Chief's Council (NPCC).

GARCIA, M. J. *The design and evaluation of physical protection systems*. 2nd. Edition. USA: Butterworth-Heinemann. 2007.

GREAT BRITAIN. Corporate Manslaughter and Corporate Homicide Act 2007. London: TSO.

GREAT BRITAIN. Data Protection Act 1998. London: TSO.

GREAT BRITAIN. Health and Safety at Work etc. Act 1974. London: Her Majesty's Stationery Office.

GREAT BRITAIN. The Fraud Act 2006. London: TSO.

GREAT BRITAIN. The Bribery Act 2010. London: TSO.

ISO 28000, *Specification for security management systems for the supply chain.*

ISO/DTS 22318, *Societal Security – Business continuity management – Guidance for supply chain continuity.*

JEFFRY, A. *Crime prevention through environmental design*. UK: Sage. 1971.

MARTIN, C. *Understanding Supply Chain Risk: a self-assessment workbook*. Bedford: Cranfield University School of Management/ Wetherby: Department of Transport Publications. 2009.

PAS 555, *Cyber security risk – Governance and management – Specification.*

PAS 1998, *Whistleblowing arrangements – Code of practice.*

TALBOT, J. and JAKEMAN, M. *Security Risk Management: Body of Knowledge*: Vol. 69, Wiley Series in Systems Engineering and Management. UK: Wiley. 2009.

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™