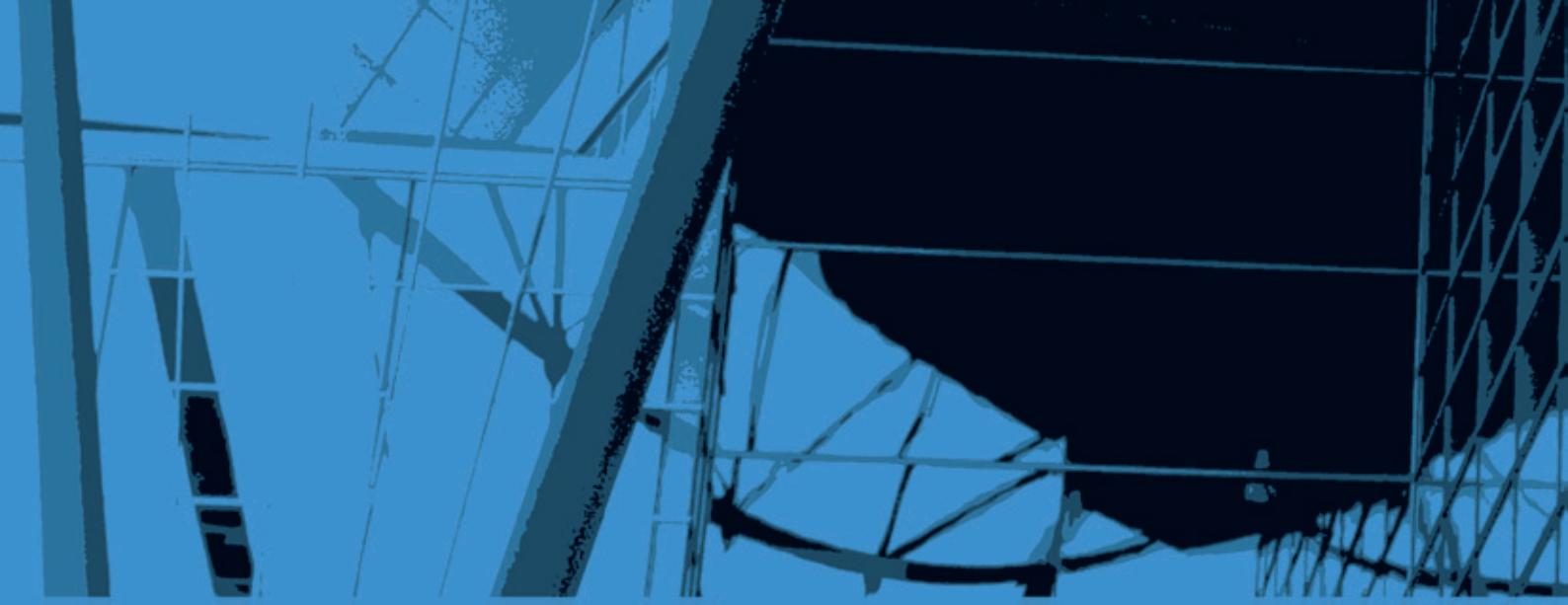


PAS 555:2013

Cyber security risk – Governance and management – Specification

CISCO

Control Risks

PA Consulting Group

Symantec

G4S

bsi.

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2013. Published by BSI Standards Limited 2013.

ISBN 978 0 580 78755 3

ICS 35.040

No copying without BSI permission as permitted by copyright law.

Publication history

First published May 2013

Contents

© The British Standards Institution 2013

© The British Standards Institution 2013

Foreword

This PAS was sponsored by the Cyber Alliance (comprising Cisco, Control Risks, G4S, PA Consulting Group and Symantec). Its development was facilitated by BSI Standards Limited and is published under licence from The British Standards Institution. It came into effect on 31 May 2013.

Acknowledgement is given to the technical author Grace Shacklady (of G4S) and to the following organizations involved in the development of this specification as members of the steering group:

- 3SDL
- Association of British Certification Bodies
- Bird & Bird
- BP plc
- Control Risks
- Department for Business, Innovation and Skills
- G4S
- King's College London
- Information Security Forum
- Intellect
- Leading Edge Forum
- Mike StJohn Green Consulting Ltd
- PA Consulting Group
- Roke Manor Research
- The Security Institute

Acknowledgement is also given to those individuals and organizations that submitted comments during the public consultation.

The British Standards Institution retains ownership and copyright of this PAS. BSI Standards Limited as the publisher of the PAS reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in *Update Standards*.

Relationships with other publications

This PAS is intended to be used as a stand-alone specification, or it can be used as a companion to other relevant standards, by any organization that wishes to have confidence in its cyber security.

The requirements of this PAS define the overall outcomes of effective cyber security. These outcomes can be achieved in a variety of ways, which are not specified here. However Annex A provides an illustration of how other relevant standards can deliver the requirements of this PAS. It should be noted, however, that the list in Annex A is not exhaustive or prescriptive and there may be other standards which are more specific to an organization's business.

The PAS specifically targets top management of an organization and intentionally has broad coverage in terms of its requirements. It does not intend to replace existing, well-established standards but provides a potential framework for understanding the outcomes of other standards in a specific cyber security context.

Use of this document

As a specification document, this PAS provides a set of absolute requirements (also referred to as outcomes), each objectively verifiable; none of the requirements is optional.

There is no implied implementation order within this PAS. Organizations can choose how they address each clause according to their business scope, assessed risk and risk appetite.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is "shall".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element. For some clauses, introductory text is provided in a shaded box to provide additional context and information about that clause.

The word "should" is used to express recommendations, the word "may" is used to express permissibility and the word "can" is used to express possibility, e.g. a consequence of an action or event.

Spelling conforms to *The Shorter Oxford English Dictionary.*

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 PAS cannot confer immunity from legal obligations.

© The British Standards Institution 2013

Executive summary

Overview

PAS 555 intends to define the outcomes of effective cyber security by providing a framework that enables understanding of the broad scope of the capabilities required. Importantly it emphasizes that technical measures alone are not enough – effective outcomes encompass people and behaviours, physical and equipment security, as well as governance, leadership and culture.

The framework does not comprise a simple cycle of events, more a mesh of interdependent activities, so that an organization's cyber security integrates people, IT/technical and intelligence, detection, investigation and learning elements from across the organization. It does not specify the actions and processes that an organization can follow in order to achieve the outcomes – this is for the organization to decide.

PAS 555 is aimed at every organization, regardless of size. It identifies what good cyber security looks like, while providing the flexibility for organizations to identify how best to achieve the outcomes in a way that is appropriate to their business. It is designed to be scalable and so is suitable for use by SMEs, not-for-profit organizations and the largest international companies alike.

Benefits

The key benefits of implementing PAS 555 are:

- improved likelihood of **achieving objectives**;
- improved stakeholder **confidence and trust**;
- enhanced business **reputation and competitive advantage**.

Applying PAS 555 can enable an organization to, for example:

a) focus investment in the most appropriate way;
b) minimize potential losses;
c) improve operational effectiveness and efficiency;
d) improve organizational resilience;
e) improve loss prevention and incident management;
f) improve controls;
g) improve organizational learning;
h) improve awareness of the need to identify and mitigate cyber security risk throughout the organization.

Outcomes of PAS 555

The benefits outlined can be realized by complying with the requirements (outcomes) described in this specification (and illustrated in Figure 1):

Management structure: Effective structures and organization that manage cyber security risk according to business scope, assessed risk and risk appetite.

Commitment to a security culture: Starts with members of top management as role models and encourages the right behaviours throughout the organization to enable improved cyber security.

Security context: Balances cyber security risks alongside other comparable risks and the organization's overall business objectives.

Business architecture strategy: Cyber security is an integral part of the through-life management of the organization, its systems processes and structures, in accordance with assessed risk.

Capability development strategy: Training and development that enables everyone to deliver their role in effective cyber security.

Supplier and partner strategy: Extends cyber security defences across the whole supply chain.

Technology strategy: Embeds cyber security into procurement and the life-cycle management of hardware, software and other equipment.

Business resilience: A level of resilience against cyber attack commensurate with the services it provides, its assessed risk, and risk appetite.

Compliance with legislation and other standards: Identifies, understands and is compliant with legislation and adopted standards relevant to the business sector and the services that the organization provides.

Risk assessment: Identifies and understands assets and the threats to and vulnerabilities of those assets so that these can be minimized, mitigated or managed in a timely manner in accordance with the organization's business scope and risk appetite.

© The British Standards Institution 2013

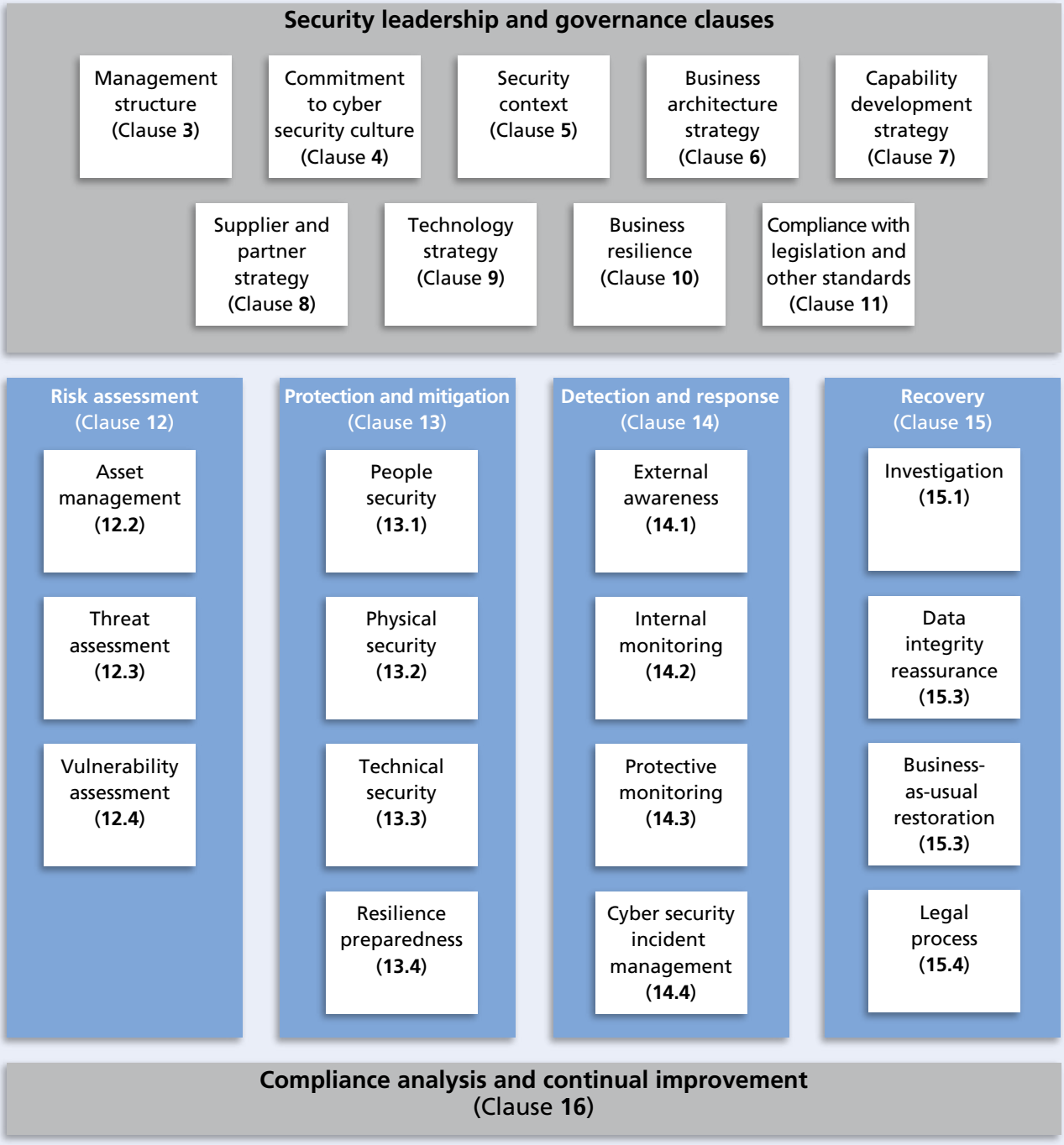
Protection and mitigation: Understands and minimizes threats from both within and outside the organization, and reduces the impact of any actual or potential cyber security incident.

Detection and response: Detects and recognizes threats from within and outside the organization, and the difference between incidents and anomalies versus trends.

Recovery: Stops, investigates and recovers from an attempted or successful cyber attack in a timely fashion and reviews circumstances and actions taken.

Compliance analysis and continual improvement: Establishes a "learning organization" through continual learning and improvement, which is embedded within the organization, to ensure that it is not subject to the same threats and hazards repeatedly.

Figure 1 – Key outcomes of PAS 555



NOTE There is no implied order of implementation.

© The British Standards Institution 2013

0 Introduction

0.1 Cyber security

Cyber security is a term that encompasses and extends information assurance and information technology (IT) security, both of which have been developing as concepts over the last 40 years, ever since the first computer virus was described in 1972. Almost every organization relies on cyberspace, with most business assets linked to it in some way. It is not only IT assets that have network connectivity, for example photocopiers, telephone systems, building control systems, industrial process control and manufacturing plants are now vulnerable to remote attack.

The business assets that are now exposed range from corporate data to customer data, intellectual property, and even the brand and reputation of an organization. Therefore, threats to cyber security present a critical challenge to organizations in terms of scale, complexity and potential impact.

0.2 Risk and resilience

PAS 555 sets out to define good cyber security in the context of risk, where the risk is managed and addressed commensurate with an organization's business scope, assessed risk and risk appetite. Its use will support an organization to prepare itself in order to optimize its defence against, response to and recovery from any cyber security incident.

0.3 An outcome-based standard

Many cyber security standards and guidelines are available. They tend to define good practice as to *how* elements of effective cyber security might be achieved. For example, BS ISO/IEC 27001, or guidelines such as the *Critical controls for effective cyber defense* [1], the *10 Steps to cyber security: Executive companion* [2] and *ISF's Standard of Good Practice* [3]. However, the challenge presented by rapid changes in technology and how cyberspace is exploited means that the way in which any particular security objective is achieved will also need to adapt rapidly.

PAS 555 instead defines the fundamental set of outcomes that these controls, systems and processes aim to achieve. As a result, they are less likely to change over time whereas the way in which the outcomes are achieved can change and develop. This specification also applies to the whole enterprise and its supply chain, avoiding the dangers that can arise when the scope of security measures covers only part of the business.

While a freedom of choice in the *how* is provided, this does not mean that there is an option to be less than robust in the interpretation and application of PAS 555; the outcomes can only be achieved through good practice. Nonetheless, what is appropriate good practice for a large organization may be inappropriate for a smaller one. Scenarios that illustrate how different types of organization can deal with cyber security risk using PAS 555 are given in Annex B.

0.4 Convergence

PAS 555 is not a simple cycle of events, more a mesh of interdependent activities; so that an organization's cyber security integrates physical, IT/technical and intelligence, detection and investigation and learning elements from across the organization.

0.5 Claims of compliance

A claim of compliance can be made on the basis of:

a) a first-party compliance assessment performed by the organization (self-assessment);

b) a second-party compliance assessment performed by, for example, a relevant trade association; or

c) a third-party compliance assessment performed by an organization, such as a certification body, that is independent of both the organization responsible and, for example, a relevant trade association.

NOTE *An organization can claim direct compliance with PAS 555 (i.e. when it is used alone and not alongside other standards), or compliance by using it in conjunction with an existing management system standard where an existing management system standard can help an organization comply with some of the requirements of PAS 555 (see Annex A for an illustration of how a selection of other standards can deliver the outcomes of this PAS).*

© The British Standards Institution 2013

1 Scope

This PAS specifies a framework for the governance and management of cyber security risk.

The requirements of this PAS define the overall outcomes of effective cyber security, and include technical, physical, cultural and behavioural measures alongside effective leadership and governance.

While there are many standards and guidelines available that can help tackle cyber security risk, they tend to define good practice as to how elements of effective cyber security might be achieved. PAS 555 does not specify such processes or actions – it allows any organization to choose how it achieves the specified outcomes, whether that be through the adoption of other standards and management systems, such as BS ISO/IEC 27001, or through its own defined processes.

Since the PAS 555 framework defines the outcomes of effective cyber security, it is less likely to change over time whereas the way in which the outcomes are achieved can change.

The PAS is intended for any organization that wishes to establish confidence in its cyber security governance and management. It is applicable to all organizations regardless of their size, type and the nature of their business.

2 Terms and definitions

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

2.1 assessment

examination to determine whether activities and related results conform to planned arrangements and whether these arrangements are implemented effectively and are suitable for achieving the organization's cyber security objectives

2.2 asset

anything that has value to the organization

NOTE *There are many types of assets, including:*

a) information;

b) software, such as a computer program;

c) physical, such as a computer;

d) services;

e) people, and their qualifications, skills, and experience; and

f) intangibles, such as reputation and image.

[SOURCE: BS ISO/IEC 27000:2012, **2.4**]

2.3 business architecture

blueprint of an organization's business structure that is used to align strategic objectives and tactical demands

2.4 business as usual (BAU)

normal execution of organizational operations either by a team or an individual

2.5 compliance

fulfilment of specified requirements

NOTE *For example, the requirements of standards and/or legislation.*

© The British Standards Institution 2013

2.6 change impact assessment

systematic approach that seeks to identify risks associated with proposed change

NOTE *Proposed change can include, for example, system configurations, operating practices, policies or procedures and any new or different activities to be performed.*

2.7 culture

predominating attitudes and behaviours that categorize the functioning of a group or organization

NOTE *For example, the attitudes and behaviours can be categorized by common values and approaches.*

2.8 cyber security

ability to protect or defend the use of cyberspace from cyber attacks

[SOURCE: CNSSI-4009]

2.9 cyber security event

identified occurrence of a system, service or network state indicating a possible breach of cyber security or failure of safeguards, or a previously unknown situation that may be security relevant

[SOURCE: ISO/IEC 27000:2012, **2.31**, modified]

2.10 cyber security incident

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

[SOURCE: ISO/IEC 27000:2012, **2.32**, modified]

2.11 cyberspace

global network of computers of which the internet is part

2.12 extended enterprise

organization and its business partners, suppliers and customers

2.13 governance

system by which organizations are directed and controlled

2.14 impact

aggregate of the evaluated possible or actual consequences of a particular outcome

2.15 incident

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

2.16 integrity

property of protecting the accuracy and completeness of assets

[SOURCE: BS ISO/IEC 27000:2012, **2.36**]

2.17 leadership

capacity to influence people, by means of personal attributes and/or behaviours, to achieve a common goal

2.18 loss

negative consequence

2.19 monitoring

determining the status of a system, a process or an activity

2.20 organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

NOTE *The concept of organization includes, but is not limited to, sole trader, company, corporation, firm, enterprise, authority, partnership, institution, charity or association, or part or combination thereof, whether incorporated or not, public or private.*

[SOURCE: BS EN ISO 9000:2005, **3.3.1**]

2.21 people security controls

measures to ensure that individuals with authorised access to controlled facilities, systems or digital assets conduct authorized activities securely

NOTE *For example, training and awareness programmes.*

© The British Standards Institution 2013

2.22 physical security controls

measures designed to prevent or detect unauthorized physical access or damage to assets

NOTE For example, fences, access-controlled doors, guards.

2.23 procedure

specified way of carrying out an activity or a process

[SOURCE: BS EN ISO 9000:2005, **3.4.5**, modified]

2.24 process

set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: BS EN ISO 9000:2005, **3.4.1**]

2.25 resilience

ability of assets, networks and systems to anticipate, absorb, adapt to and/or recover from a disruptive event or incident

2.26 resilience preparedness

anticipation, assessment, prevention and preparation for recovery after an incident

2.27 resources

all assets, people, skills, information, technology (including plant and equipment), premises and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objectives

2.28 risk

effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected – positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential events and consequences or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

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

2.29 risk appetite

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

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

2.30 risk assessment

overall process of risk analysis and risk evaluation

2.31 risk management

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

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

2.32 security context

environment in which the organization seeks to achieve its objectives

2.33 technical security controls

measures that protect against unauthorized access to digital assets

NOTE For example, username/passwords, firewalls, antivirus software.

2.34 through-life management

coherent and holistic approach to managing the whole-life costs and outlook across equipment or the life cycle of a project or programme

2.35 top management

person or group of people who directs and controls an organization at the highest level

NOTE For example, in some organizations this may be "the board" (i.e. a group of people who officially administer a company, trust, etc.).

[SOURCE: BS EN ISO 9000:2005, **3.2.7**, modified]

© The British Standards Institution 2013

3 Management structure

The top management shall have a structure to manage its cyber security risk commensurate with the organization's business scope, assessed risk and risk appetite.

The organization shall:

a) have an owner of cyber security within the organization at a level of seniority commensurate with the size and scope of the organization and the exposure to cyber security risk;

b) clearly define and allocate cyber security responsibilities, authority and resources within the organization.

4 Commitment to a cyber security culture

The organization's top management shall define and demonstrate how it engenders a culture of cyber security within the organization.

NOTE *A cyber security culture is one where values, attitudes and behaviours are the foundation of day-to-day life in an organization. It is one where being careless about (cyber) security is not acceptable. It is recognized that it will take time to achieve a culture change and cannot be immediate.*

5 Security context

The organization's top management shall address cyber security alongside all other risks and opportunities (see Clause **12**) and other business objectives.

6 Business architecture strategy

The organization shall include cyber security in the through-life management of the organization, its systems, processes and structures (across physical, technical and people) in accordance with assessed risk (see Clause **12**).

7 Capability development strategy

The organization shall have cyber security awareness programmes, training and development, so that all individuals in the extended enterprise have the awareness and competence to fulfil their cyber security role and contribute to an effective cyber security culture.

8 Supplier and partner strategy

The organization shall manage its cyber security risk across the organization and its business partners, suppliers and customers, including any interdependencies.

NOTE *A sample supplier/partner cyber security competence assessment report is provided in Annex C.*

9 Technology strategy

The organization shall:

a) include cyber security as part of the choices made in hardware, software and other equipment procurement and through their life-cycle to disposal;

b) include cyber security as part of its change impact assessment;

c) implement practices that identify new vulnerabilities from introduced or planned changes;

d) implement layers of protection to control access to assets in accordance with the assessed risk;

e) plan future changes to hardware and/or software or other equipment on the basis of taking the opportunity to enhance cyber security where the assessed risks demonstrate the need.

NOTE *The technology strategy of an organization can be dependent on its assessed risk (Clause **12**).*

10 Business resilience

The organization shall identify and implement the level of resilience it needs commensurate with the types of services it provides and the assessed risks (see Clause **12**).

11 Compliance with legislation and other standards

The organization shall:

a) identify the regulations and legislation that it needs to comply with in order to conduct its business;

b) identify the standards and guidelines that the organization could comply with to minimize its vulnerability to cyber security threats, commensurate with its risk appetite;

NOTE *Relevant standards that an organization can consider include, but are not limited to, those illustrated in Annex A.*

c) implement regulations, legislation, chosen standards and guidelines in a way that enhances cyber security.

© The British Standards Institution 2013

12 Risk assessment

An organization can choose to follow the pattern of risk analysis and management methods already in use, or prescribed by other standards, or it can choose its own sequence according to its defined security context.

12.1 General

The organization shall identify, and understand, its assets and identify the threats to and vulnerabilities of those assets so that these can be minimized, mitigated or managed in a timely manner in accordance with its business scope and risk appetite.

***NOTE** The outcomes presented in Clause **12** should be executed on an ongoing basis.*

12.2 Asset management

The organization shall identify, and understand, its assets across the business and its partners, suppliers and customers, so that:

a) assets are categorized according to their value, sensitivity and the impact of their disclosure, damage or loss;

b) assets are registered, tracked and managed in accordance with their categorization;

c) access to assets is known, understood and managed with suitable controls over who has access (in use, in storage, during transportation, configuration, etc.).

12.3 Threat assessment

The organization shall identify the actual and potential threats and hazards to assets across its various functions.

12.4 Vulnerability assessment

The organization shall identify new and existing vulnerabilities so that remediation of any susceptibilities can be carried out.

***NOTE** An environmental susceptibility could be the lack of flood defences, or unsuitable building design in regard to water storage, or it could be the lack of sufficient firewall or virus defences.*

13 Protection and mitigation

This clause looks at how an organization can take steps to mitigate the effects of threats from both within and outside the organization. It also addresses any identified weaknesses in physical security and builds an organization's resilience to reduce the impact of any cyber security incident.

13.1 People security

The organization shall identify and take steps to minimize, mitigate or manage risk to the organization posed by people from both inside and outside the organization including its business partners, suppliers and customers.

13.2 Physical security

The organization shall identify physical vulnerabilities and susceptibilities, and implement physical security controls in accordance with the risk assessment in Clause **12** and monitor access to physical facilities and equipment.

13.3 Technical security

The organization shall implement technical security controls to protect its assets.

13.4 Resilience preparedness

The organization shall build resilience preparedness into its people, processes and technology to reduce the impact of a cyber security incident.

© The British Standards Institution 2013

14 Detection and response

Top management should be able to recognize any threats to their cyber security from both within and outside the organization. They should be able to recognize incidents from trends and anomalies, and to identify all sources of such information – especially those sources that would not normally be used. Discipline should be applied to the monitoring and logging of internal and external activity, and a system developed so that incidents can be managed in a timely and effective manner if they occur.

It is important that an organization does not just gather data in isolation. Protective monitoring is intended to illustrate those various forms of information that should be looked at holistically to aid the detection of existing and new threats to cyber security, from whatever direction they come, and to encourage organizations to build their own "portfolio" of intelligence so that mitigation and management of possible threats and vulnerabilities can be undertaken.

14.1 External awareness

The organization shall collect, monitor, analyse and share (with trusted partners) information/intelligence on any new, existing or changing cyber security threats and respond in accordance with the assessed risk and nature of the business as part of regular/planned cyber risk evaluations.

14.2 Internal monitoring

The organization shall:

a) define and maintain its capability to detect that a cyber security event or incident has occurred and what action it takes in response;

b) maintain an audit trail of its internal monitoring activities and actions taken.

14.3 Protective monitoring

The organization shall determine and collect information available from diverse sources, both from within and outside the organization, that allows the identification of trends and anomalies that might indicate breaches of cyber security and inform the threat assessment (**12.3**).

14.4 Cyber security incident management

The organization shall identify how it prepares for, and is able to take command and control of, an incident and how it determines an effective response, including details of what communications, and people, technical and physical security measures might be required.

15 Recovery

With cyber attacks and their sophistication on the increase, no organization can assume that it is immune. This clause outlines what an organization can have in place to stop, investigate and recover from any attempted or successful cyber attack in a timely manner and to review circumstances and actions taken.

15.1 Investigation

The organization shall demonstrate a capability to investigate and document cyber security events and incidents to enable learning, review and identification of good practice and to support any legal case or other follow up.

15.2 Data integrity reassurance

The organization shall define and maintain its capability to restore the integrity of the organization's assets following a cyber security incident.

15.3 Business-as-usual restoration

The organization shall demonstrate its ability to restore "business as usual" following a cyber security incident, in a timely manner and consistent with the damage done/being done to itself, its partners, suppliers and customers.

15.4 Legal process

The organization shall identify and manage its legal and regulatory obligations in respect of cyber security, and consider its requirements for the availability of legal advice to minimize further damage in the event of an incident.

16 Compliance analysis and continual improvement

An organization could have all other elements of this PAS in place. However, unless there is continual learning, and improvement is embedded within the organization, it could be subject to the same threats and hazards repeatedly. The intention of this clause is the establishment of a "learning organization".

The organization shall demonstrate how it learns from and improves its cyber security and resilience position so it can respond to developing and dynamic (active) threats and hazards.

© The British Standards Institution 2013

Annex A (informative)
Achieving compliance with PAS 555

Table A.1 gives an illustration of how a selection of other standards can deliver the requirements described in this PAS.

The table is provided to facilitate an integrated approach to implementation of relevant standards and ensure that cyber security is referred to when addressing the component parts of these standards. The table can also aid the inclusion of cyber security into an existing management system.

__NOTE__ The relationships shown between this PAS and other standards and guidelines should not be construed as equivalent. Compliance with PAS 555 does not guarantee compliance with similar clauses in other standards. Users are referred to __0.5__ for guidance on making claims of compliance.

Table A.1 – Achieving compliance with PAS 555: a selection of other standards

PAS 555 clause	PAS 555 outcome	BS EN ISO 9001:2008	BSI ISO/IEC 20000-1:2011	BS ISO/IEC 27001:2005	BS ISO 22301:2012	BS ISO 31000:2009
3	**Management structure** The top management shall have a structure to manage cyber security risk commensurate with the organization's business scope, assessed risk and risk appetite.	5.5	4.1	5.1 A.6.1.2	5.1 5.4	4.3.3
4	**Commitment to a cyber security culture** The organization's top management shall define and demonstrate how it engenders a culture of cyber security within the organization.	5.1	4.1	5.1 A.6.1.1	5.2	4.3.1 5.2
5	**Security context** The organization's top management shall address cyber security alongside all other risks and opportunities and other business objectives.	5.4	6.6	4.2.1 A.5.1.1 A.5.1.2 A.6.2	6	4.3.1
6	**Business architecture strategy** The organization shall include cyber security in the through-life management of the organization, its systems, processes and structures (across physical, technical and people) in accordance with assessed risk.	5.4	6.4 6.5	4.2.1	4	4.3.1

© The British Standards Institution 2013

Table A.1 – Achieving compliance with PAS 555: a selection of other standards *(continued)*

PAS 555 clause	PAS 555 outcome	BS EN ISO 9001:2008	BSI ISO/IEC 20000-1:2011	BS ISO/IEC 27001:2005	BS ISO 22301:2012	BS ISO 31000:2009
7	**Capability development strategy** The organization shall have cyber security awareness programmes, training and development, so that all individuals in the extended enterprise have the awareness and competence to fulfil their cyber security role and contribute to an effective cyber security culture.	6.2	4.4.2	5.2.2 A.6.2 A.8.2.2 A.10.2	7.2	4.3.5
8	**Supplier and partner strategy** The organization shall manage its cyber security risk across the organization and its business partners, suppliers and customers, including any interdependencies.	7.4	7.2	A.6.2 A.10.2		4.3.7 5.3.2
9	**Technology strategy** The organization shall: a) include cyber security as part of the choices made in hardware, software and other equipment procurement and through the life-cycle to disposal; b) include cyber security as part of its change impact assessment; c) implement practices that identify new vulnerabilities from introduced or planned changes; d) implement layers of protection to control access to assets in accordance with the assessed risk; e) plan future changes to hardware and/or software or other equipment on the basis of taking the opportunity to enhance cyber security where the assessed risks demonstrate the need.	7.4	5.1 to 4	A.12		4.3.1

© The British Standards Institution 2013

Table A.1 – Achieving compliance with PAS 555: a selection of other standards *(continued)*

PAS 555 clause	PAS 555 outcome	BS EN ISO 9001:2008	BSI ISO/IEC 20000-1:2011	BS ISO/IEC 27001:2005	BS ISO 22301:2012	BS ISO 31000:2009
10	**Business resilience** The organization shall identify and implement the level of resilience it needs commensurate with the types of services it provides and the assessed risk.		6.3 8	A.14.1	6.2 7.1	4.3.5
11	**Compliance with legislation and other standards** The organization shall identify the regulations and legislation that it needs to comply with in order to conduct its business; and the standards and guidelines that the organization could comply with to minimize its vulnerability to cyber security threats…	4.1	4.5	4.2.1 A.15.1 A.15.2 A.15.3	9.1	4.3.1 4.3.2
12.1	**Risk assessment** The organization shall identify, and understand, its assets and identify the threats to and vulnerabilities of those assets so that these can be minimized, mitigated or managed in a timely manner in accordance with business scope and risk appetite.		6.6	4.2.1d) to g)	6.1 8.2.1	5.4
12.2	**Asset management** The organization shall identify, and understand, its assets across the business and its business partners, suppliers and customers so that they are categorized, registered and access to assets is known, understood and managed.		6.6	4.2.1d)	8.2.3	
12.3	**Threat assessment** The organization shall identify the actual and potential threats and hazards to assets across its various functions.		6.6	4.2.1d)		5.4.2

© The British Standards Institution 2013

Table A.1 – Achieving compliance with PAS 555: a selection of other standards *(continued)*

PAS 555 clause	PAS 555 outcome	BS EN ISO 9001:2008	BSI ISO/IEC 20000-1:2011	BS ISO/IEC 27001:2005	BS ISO 22301:2012	BS ISO 31000:2009
12.4	**Vulnerability assessment** The organization shall identify new and existing vulnerabilities so that remediation of any susceptibilities can be carried out.		6.6	4.2.1d)		5.4.2
13.1	**People security** The organization shall identify and take steps to minimize, mitigate and manage risk to the organization posed by people from both inside and outside the organization including its business partners, suppliers and customers.		4.4.2 7.2	5.2.2 A.8	7.2 7.3	
13.2	**Physical security** The organization shall identify physical vulnerabilities and susceptibilities, and implement physical security controls in accordance with the risk assessment and monitor access to physical facilities and equipment		6.6.2	4.2.1d) to g) 5.2.1d) A.9		
13.3	**Technical security** The organization shall implement technical security controls to protect its assets		6.6.2	A.9 A.10.4 A.10.8 A.11		
13.4	**Resilience preparedness** The organization shall build resilience preparedness into its people, processes and technology to reduce the impact of a cyber security incident		6.3 8	A.14	6.2 7.2 7.3	5.5.3
14.1	**External awareness** The organization shall collect, monitor and analyse information/intelligence on any new, existing or changing cyber security threats and respond in accordance with the assessed risk and nature of the business as part of regular/planned cyber risk evaluations			A.6.2		5.3.2 5.6

© The British Standards Institution 2013

Table A.1 – Achieving compliance with PAS 555: a selection of other standards *(continued)*

PAS 555 clause	PAS 555 outcome	BS EN ISO 9001:2008	BSI ISO/IEC 20000-1:2011	BS ISO/IEC 27001:2005	BS ISO 22301:2012	BS ISO 31000:2009
14.2	**Internal monitoring** The organization shall define and maintain its capability to identify that a cyber security event or incident has occurred and what action it takes in response; and maintain an audit trail		6.6.2	A.10.1 A.10.10 A.11 A.12		5.3.3 5.6
14.3	**Protective monitoring** The organization shall determine and collect information available from diverse sources, both from within and outside the organization that allows the identification of trends and anomalies that might indicate breaches of cyber security and inform the threat assessment	Not specifically dealt with by other standards.				
14.4	**Cyber security incident management** The organization shall identify how it prepares for, and is able to take command and control of, an incident and how it determines an effective response, including details of what communications, and people, technical and physical measures might be required		6.6.3	A.13 A.14	8.4	
15	**Recovery**		6.3.2	A.13 A.14	8.4.5	
15.1	**Investigation** The organization shall demonstrate a capability to investigate and document cyber security events and incidents to enable learning, review and identification of good practice to support any legal case or other follow up	4.2.3 4.2.4	4.5.5.1	4.3.2 4.3.3 A.13 A.14		
15.2	**Data integrity reassurance** The organization shall define and maintain its capability to restore the integrity of the organization's assets following a cyber security incident		6.3.2	A.14.1	8.4	

© The British Standards Institution 2013

Table A.1 – Achieving compliance with PAS 555: a selection of other standards *(continued)*

PAS 555 clause	PAS 555 outcome	BS EN ISO 9001:2008	BSI ISO/IEC 20000-1:2011	BS ISO/IEC 27001:2005	BS ISO 22301:2012	BS ISO 31000:2009
15.3	**Business-as-usual restoration** The organization shall demonstrate its ability to restore "business as usual" following a cyber security incident, in a timely manner and consistent with the damage done/being done to itself, its partners and customers		8	A.13.2 A.14	8.4	
15.4	**Legal process** The organization shall identify and manage its legal and regulatory obligations in respect of cyber security, to minimize further damage in the event of an incident	4.2.3 4.2.4		4.3.4 4.3.3 A.13.2.3		
16	**Compliance analysis and continual improvement** The organization shall demonstrate how it learns from and improves its cyber security and resilience position so it can respond to developing and dynamic (active) threats	8.5	4.5.4	4.2.3 6 7 A.15	9 10.2	4.5 5.6

© The British Standards Institution 2013

Annex B (informative)
PAS 555 application scenarios

B.1 General

These scenarios provide examples of how PAS 555 can be used by different types of organizations and illustrate the flexibility of the PAS.

B.2 Outcome focus

Acme plc is a major manufacturer that integrates the products of many small specialist companies. It chose to implement PAS 555 to give confidence in its approach to cyber security, without prescribing how each company had to achieve the outputs.

Acme has already implemented an information security management system in a rigorous way and so can already deliver many of the outcomes that PAS 555 requires. There remained work to do around the leadership and governance outcomes and putting in procedures to recover from incidents.

Other than that Acme found that complying with PAS 555 was straightforward. However, the policies and process that suited a large company like Acme were not appropriate for some of the SMEs that were integrated with Acme. They instead chose to deliver the outcomes in alternative ways that minimized paperwork. For example, one company, which bought in its ICT services, was simply able to include many of the outcomes as requirements in its contract with its service provider. Another chose to host its data on a secure cloud rather than on its own, dated servers.

B.3 Incomplete scope

The head office of XYZ plc has a certified information security management system (ISMS) in place. The Chief Executive proudly points to the certificate whenever questioned on how he secures the company. However, at XYZ's regional office, an important client visits to discuss a new contract. The client is alarmed at how easily he could walk into the offices unchallenged and find all manner of tell-tale signs of poor security controls and awareness.

The apparent disparity in security is because the scope of the ISMS was deliberately limited to head office operations to achieve the compliance more readily. In working to achieve PAS 555, the scope extends to the whole organization, and so XYZ had quite a lot to do.

B.4 Lifecycle approach

ABC Ltd is a financial services firm. Being a financial organization it knows that it is an attractive target for cybercrime and that some attacks will be successful. It is also aware that being 100% secure is an unrealistic and costly target.

ABC chose to implement PAS 555 as it found the lifecycle approach from Assess > Protect > Respond > Recover useful in making sure appropriate effort was given to both preventing an incident and recovering from one. As such it liked the focus that PAS 555 pays to respond and recover from an incident and not just prevent one. PAS 555 recognizes that modern day cyber threats are sufficiently advanced that just as much attention should be placed on dealing with an attack as trying to prevent one.

B.5 Focus on security in context

EFG plc is an international pharmaceutical organization. EFG's operations are split in two: a small but important research facility and a range of commercial distribution offices around the world. The research facility has sensitive assets facing serious threats. The distribution offices have very little sensitive information and therefore are at low risk.

PAS 555 has a strong focus on assessing the assets to protect and the threats against them, which will be especially important for EFG's research facility. PAS 555 specifically ensures that the value of EFG's assets corresponds to the level of protection expected. This security in context approach is efficient as it means expensive security controls are only applied where they are most needed. Understanding these risks allows EFG to view cyber security risks alongside other organizational risks and manage them appropriately.

© The British Standards Institution 2013

Annex C (informative)
Sample supplier/partner cyber security competence assessment report

***NOTE** This sample report relates to Clause **8** and gives an indication of the kind of information that an organization can ask of a supplier/partner in order to provide assurance on how they manage cyber security risk.*

A contracting organization can also be asked by a supplier/partner to provide information of this kind before any contract is agreed.

The organization producing the report can adapt this sample report to suit their requirements. The report provides some recommended core text as well as guidance (shown in italics) on what information an organization might request/supply.

[***Organization name***]

Supplier/partner cyber security competence assessment report

Prepared for

Name and address for supplier being assessed.
Self-assessed or third-party assessed?

Disclaimer

***NOTE** An organization's legal team might want to include some disclaimer text to accompany this assessment.*

Introduction

Security is the shared responsibility of all involved in the cooperative, supplier activity and partnership arrangements and any breach may not only threaten company and customer assets but could compromise the security of the entire enterprise network. Those responsible for devising cyber security risk; the implementation of governance and management of cyber security play a crucial role in up-holding the integrity of the system, not only across their own business, but also with partners and suppliers.

It is essential that every enterprise is included in providing evidence of competence to others which may depend on their own security for continued and successful operation.

***NOTE** An organization should include the scope of this report in the introduction (to ensure that it covers physical, technical and people security).*

© The British Standards Institution 2013

Executive summary

[*Organization name*] are proactive in their approach to cyber security risk management and aim to achieve [*certification/a commonly accepted standard of alignment*].

It is important that [*Organization name*] and its associated asset categories remain well protected from cyber security incidents. A determination by [*organization name*] to achieve a secure business partner and [*certification of a commonly accepted standard of alignment*] status demonstrates further the emphasis it places on reducing security risk within the supply chain and partnership approach.

At [*time, date, place*] a cyber security risk assessment was conducted at [*organization, name and address*] to establish the current measures and procedures in place which can help to meet the specification contained in the Standard.

This report provides a detailed account of the current security measures at the time of the assessment and an evaluation is made in relation to the effectiveness of those measures together with other controls to reduce the risk of conducting business with the [*company/organization/individual*].

Assessment summary

Explanation of the site and how the assessment was conducted.

The assessment has identified areas that require attention and provides recommendations for improvement in relation to the following:

List elements of the cyber security risk governance and management processes that require attention as they may not meet the specification.

Overview of [*organization*]

Provide high-level information on the organization and its activities (one or two paragraphs).

Overview of site operations of [*name of organization*]

Provide a summary of the organization's site (site specific/local level). Photographs and illustrations to explain complex site operations/activities can be used.

© The British Standards Institution 2013

Risk analysis

Provide an overview of the threats and hazards to the organization:

a) in the vicinity of the organization's premises and immediate region (for example, this can include a CAP Index report and, for comparison, local police reported crime figures);

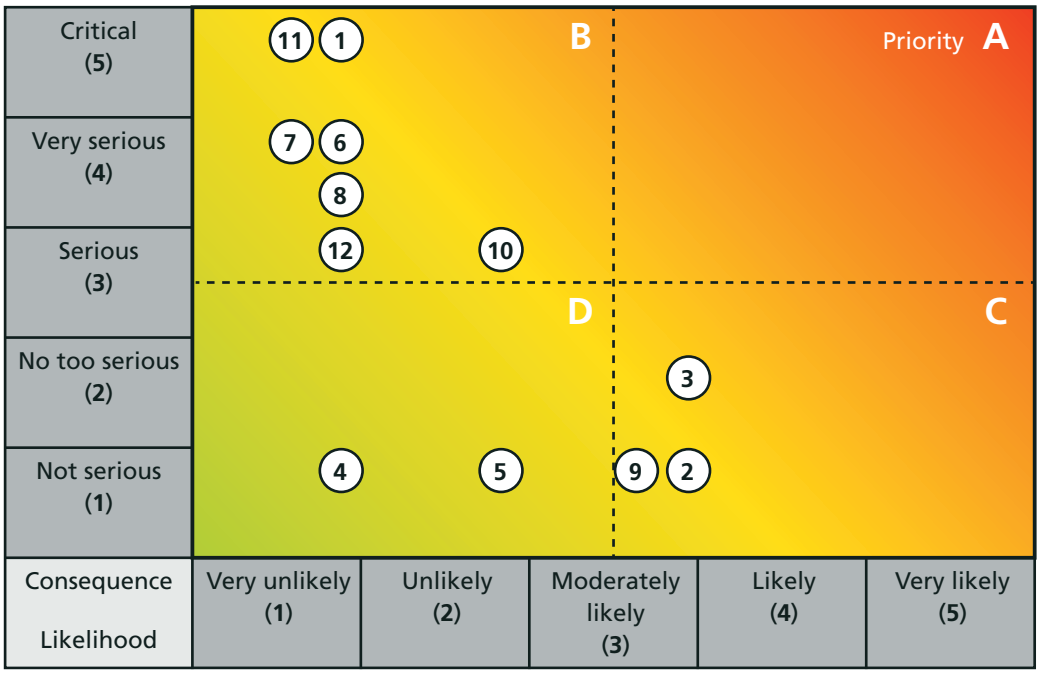
b) internal crime threats from staff;

c) importance of local criminal activity towards the site as a target;

d) environmental hazards, e.g. situation of the organization in relation to a river.

Figure C.1 provides an example of how threats and their potential impact can be illustrated.

Figure C.1 – Risk impact matrix



Key	Threat scenario		Threat scenario		Threat scenario
1	Terrorism	5	External theft	9	Lower level crime threats
2	Site intrusion/trespass	6	Smuggling of illicit goods	10	Non-compliance[1)]
3	Intrusion – break-in	7	Tampering with goods	11	Fire/arson
4	Internal theft	8	Contamination of product	12	Sabotage[2)]

[1)] Non-compliance with safety and security policies could expose the site to increased security risk.

[2)] Deliberate damage to the operating or manufacturing processes as a result of a malicious, disgruntled employee or other.

When analysing the above risk ratings, it is important to note that existing controls may not reduce both the likelihood and impact of a potential event.

© The British Standards Institution 2013

Cyber security competence assessment

The information you provide will be used to assess the cyber security competence of [*name of organization*]. Please include as much detail as possible.

NOTE *The following questions should be tailored to meet the size and needs of the organization being assessed.*

Explain the governance, leadership and culture and management structure of your organization. Provide a diagram if necessary.

Response:

Comment:

How is cyber security management implemented in your organization?

Response:

Comment:

© The British Standards Institution 2013

How does your organization conduct compliance analysis and continual improvement of your cyber security resilience?

Response:

Comment:

C.1 Report author

Provide information on the author of this report and their experience/skills.

© The British Standards Institution 2013

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.

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

BS EN ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

BS EN ISO 9001:2008, *Quality management systems – Requirements*

BS ISO/IEC 20000 1:2011, *Information technology – Service management – Part 1: Service management system requirements*

BS ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

BS ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

BS ISO 22301:2012, *Societal security – Business continuity management systems – Requirements*

BS ISO 31000:2009, *Risk management – Principles and guidelines*

CNSSI-4009:2010, *National information assurance (IA) glossary*

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

Other publications

[1] CSIS. Top 20 critical security controls for cyber defense, version 4.1, 2013. www.sans.org/critical-security-controls/cag4-1.pdf

[2] CESG, BIS and CPNI. 10 steps to cyber security: Executive companion, London: Stationery Office, 2012. www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

[3] Information Security Forum. *Standard of good practice for information security*, 2012.

© The British Standards Institution 2013

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

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

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similarly for PASs, please notify BSI Customer Services.

Tel: +44 (0)845 086 9001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)845 086 9001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop**. In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)845 086 9001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)845 086 9001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **http://shop.bsigroup.com/bsol**

Further information about British Standards is available on the BSI website at **www.bsigroup.com/standards**

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Department.

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

© The British Standards Institution 2013

This page deliberately left blank.

© The British Standards Institution 2013

This page deliberately left blank.

© The British Standards Institution 2013

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com

ISBN 978-0-580-78755-3