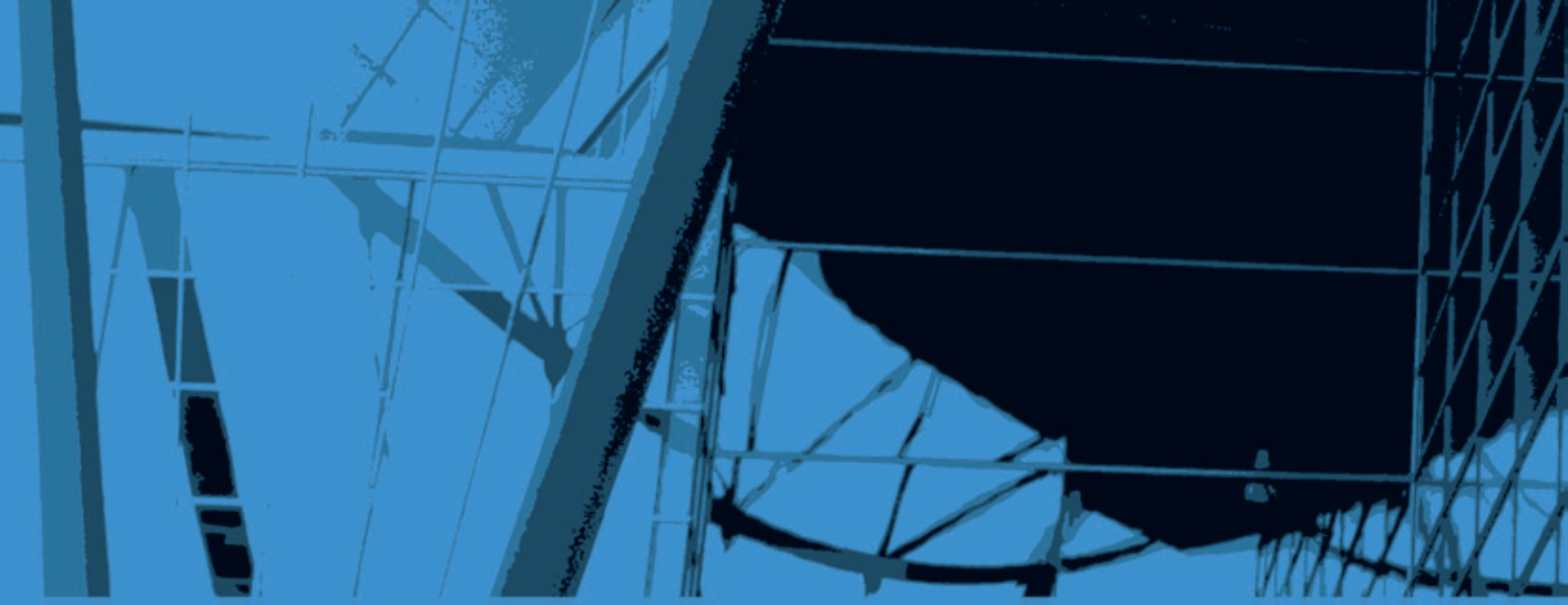


PAS 555:2013

Cyber security risk – Governance and management – Specification

CISCO

Control Risks

PA Consulting Group

Symantec

G4S

bsi.

Publishing and copyright information

ISBN 978 0 580 78755 3

ICS 35.040

Publication history

First published May 2013

Contents

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.

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.

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.

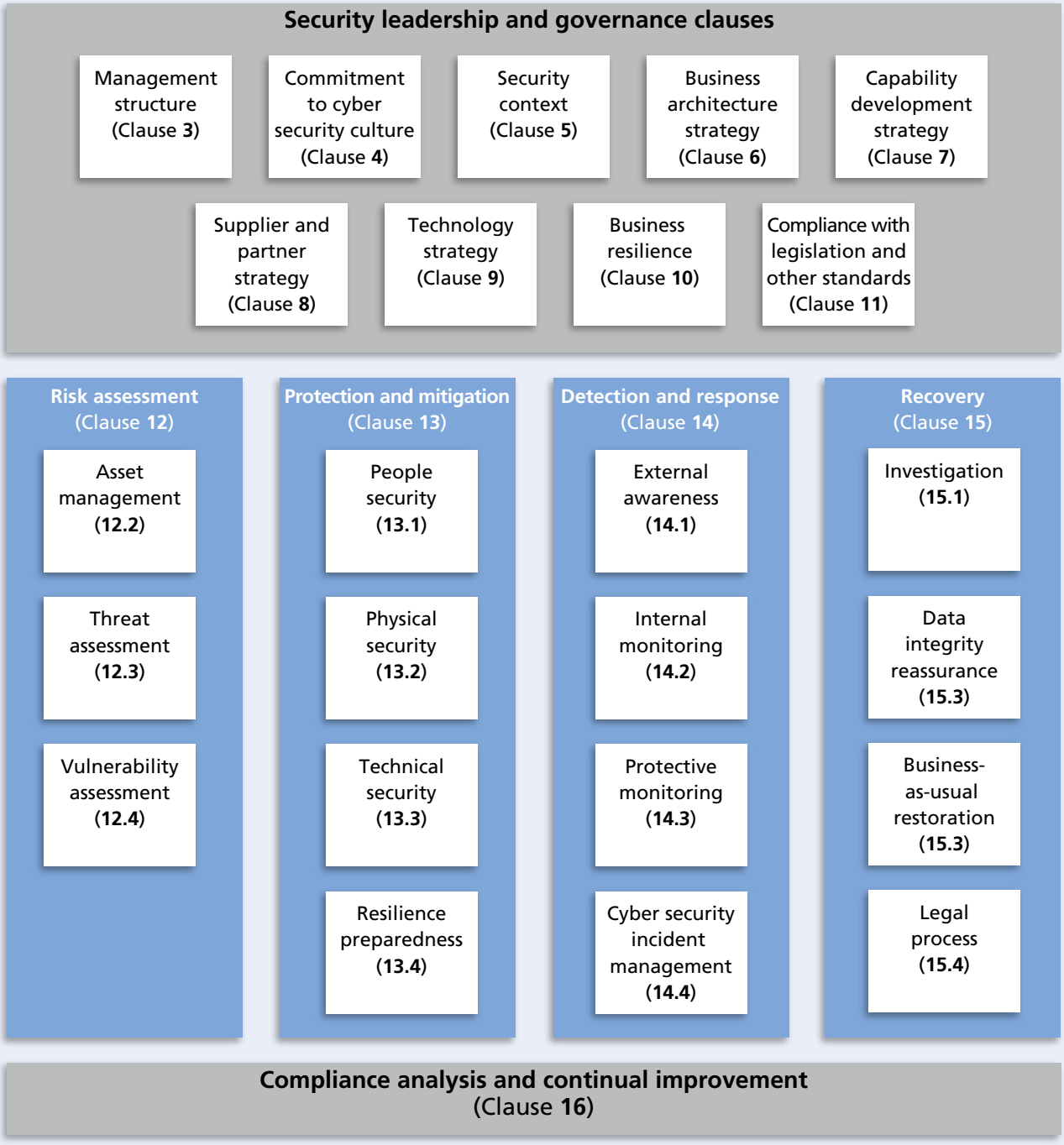
Protection and mitigation: Understands and minimizes threats from both within and outside the organization, and reduces the impact of any actual or potential cyber security incident.

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.

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).*

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.*