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.

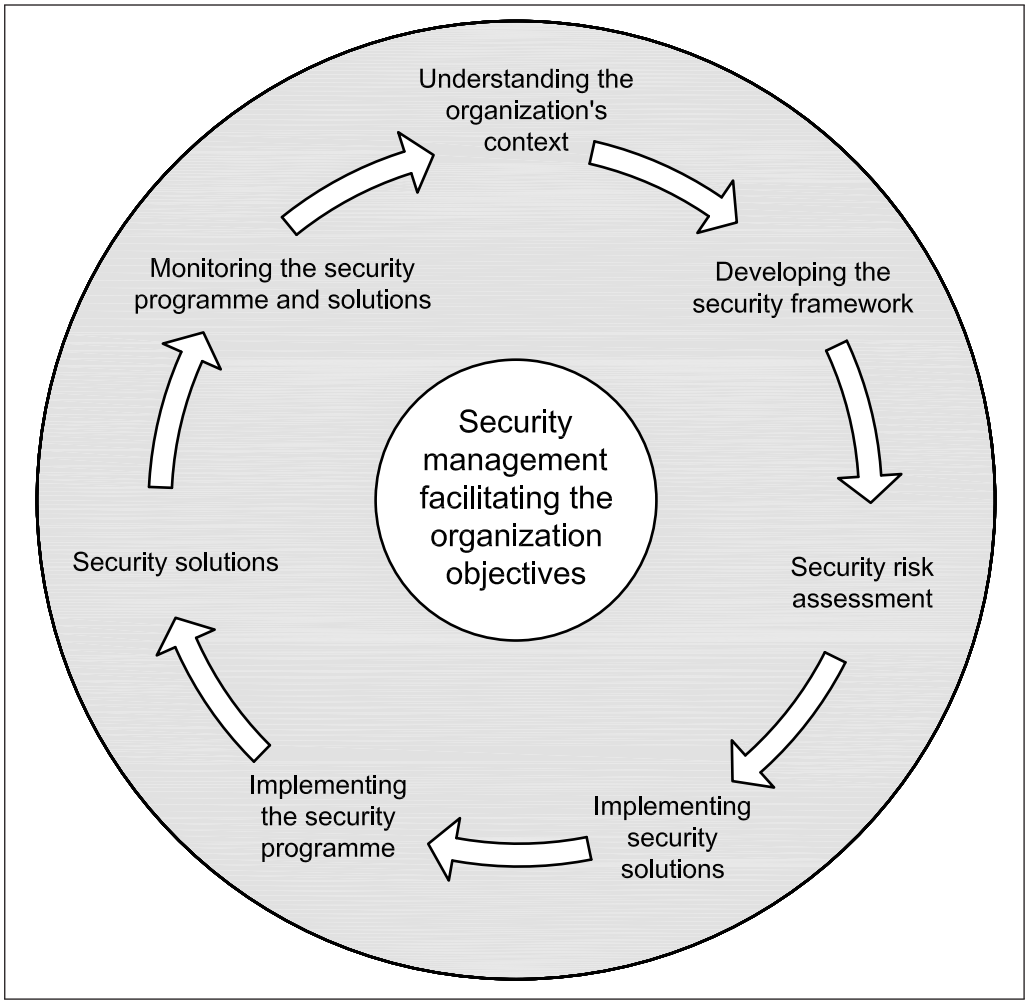
This page deliberately left blank

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